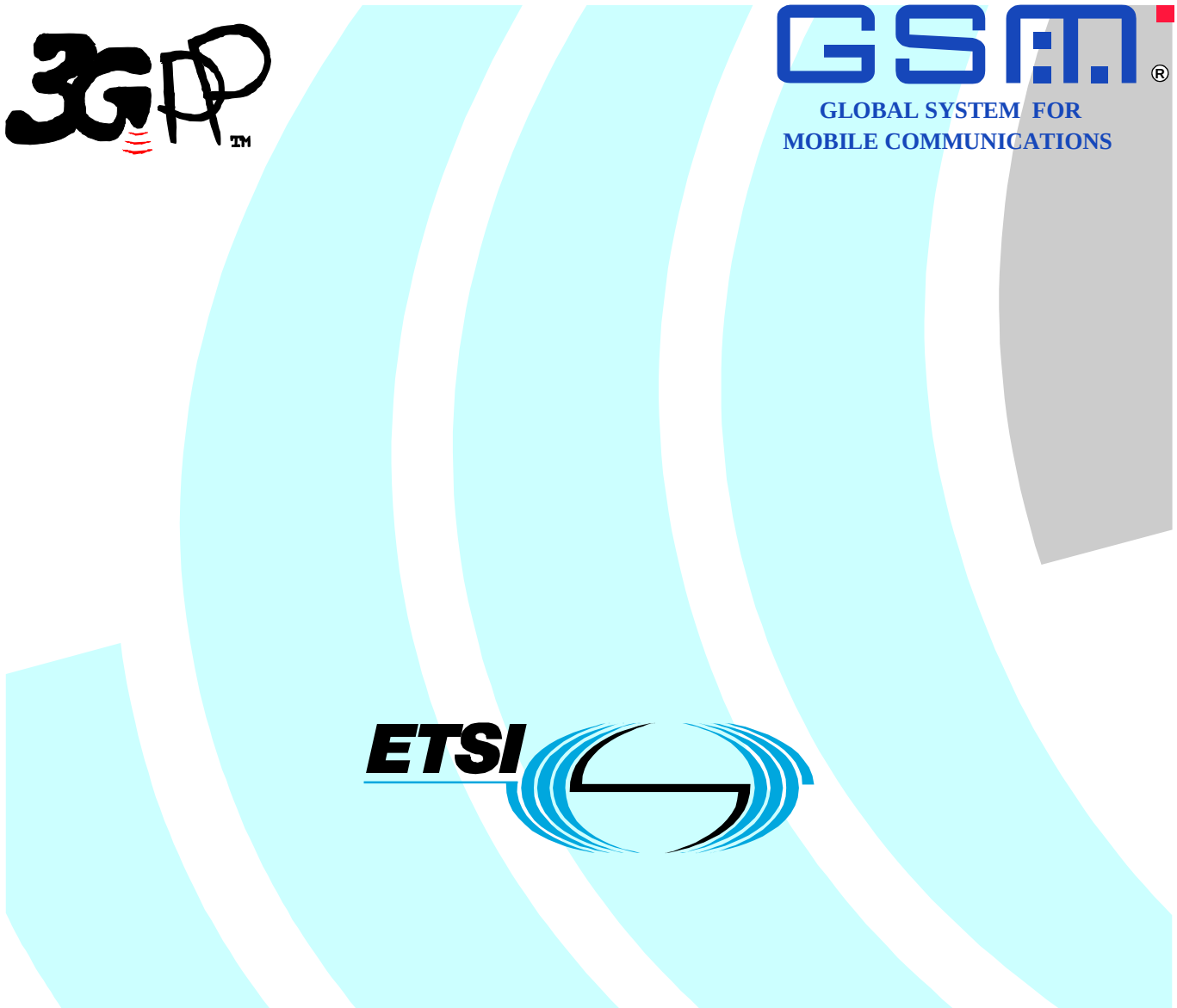
# ETSI TS 124 229 V6.10.0 (2006-03)

*Technical Specification*

**Digital cellular telecommunications system (Phase 2+);
Universal Mobile Telecommunications System (UMTS);
Internet Protocol (IP) multimedia call control protocol
based on Session Initiation Protocol (SIP) and
Session Description Protocol (SDP);
Stage 3
(3GPP TS 24.229 version 6.10.0 Release 6)**



Reference
RTS/TSGC-0124229v6a0

Keywords
GSM, UMTS

***ETSI***

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

# Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

# Foreword

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp .

# Contents

Intellectual Property Rights ..... 2
Foreword ..... 2
Foreword ..... 10
1 Scope ..... 11
2 References ..... 11
3 Definitions and abbreviations ..... 15
3.1 Definitions ..... 15
3.2 Abbreviations ..... 17
3A Interoperability with different IP-CAN ..... 19
4 General ..... 19
4.1 Conformance of IM CN subsystem entities to SIP, SDP and other protocols ..... 19
4.2 URI and address assignments ..... 20
4.2A Transport mechanisms ..... 21
4.3 Routeing principles of IM CN subsystem entities ..... 21
4.4 Trust domain ..... 21
4.5 Charging correlation principles for IM CN subsystems ..... 22
4.5.1 Overview ..... 22
4.5.2 IM CN subsystem charging identifier (ICID) ..... 22
4.5.3 Access network charging information ..... 23
4.5.3.1 General ..... 23
4.5.3.2 Access network charging information ..... 23
4.5.4 Inter operator identifier (IOI) ..... 23
4.5.5 Charging function addresses ..... 24
5 Application usage of SIP ..... 24
5.1 Procedures at the UE ..... 24
5.1.1 Registration and authentication ..... 24
5.1.1.1 General ..... 24
5.1.1.1A Parameters contained in the ISIM ..... 24
5.1.1.2 Initial registration ..... 25
5.1.1.3 Initial subscription to the registration-state event package ..... 26
5.1.1.4 User-initiated re-registration ..... 27
5.1.1.5 Authentication ..... 29
5.1.1.5.1 General ..... 29
5.1.1.5.2 Network-initiated re-authentication ..... 30
5.1.1.5.3 Abnormal cases ..... 30
5.1.1.5A Change of Ipv6 address due to privacy ..... 31
5.1.1.6 User-initiated deregistration ..... 31
5.1.1.7 Network-initiated deregistration ..... 32
5.1.2 Subscription and notification ..... 33
5.1.2.1 Notification about multiple registered public user identities ..... 33
5.1.2.2 General SUBSCRIBE requirements ..... 33
5.1.2A Generic procedures applicable to all methods excluding the REGISTER method ..... 33
5.1.2A.1 Mobile-originating case ..... 33
5.1.2A.2 Mobile-terminating case ..... 34
5.1.3 Call initiation - mobile originating case ..... 35
5.1.3.1 Initial INVITE request ..... 35
5.1.4 Call initiation - mobile terminating case ..... 36
5.1.4.1 Initial INVITE request ..... 36
5.1.5 Call release ..... 37
5.1.6 Emergency service ..... 37
5.1.7 Void ..... 37
5.2 Procedures at the P-CSCF ..... 37

5.2.1 General....37
5.2.2 Registration....38
5.2.3 Subscription to the user's registration-state event package....41
5.2.4 Registration of multiple public user identities....42
5.2.5 Deregistration....43
5.2.5.1 User-initiated deregistration....43
5.2.5.2 Network-initiated deregistration....43
5.2.6 General treatment for all dialogs and standalone transactions excluding the REGISTER method....44
5.2.6.1 Introduction....44
5.2.6.2 Determination of mobile-originated or mobile-terminated case....44
5.2.6.3 Requests initiated by the UE....44
5.2.6.4 Requests terminated by the UE....47
5.2.7 Initial INVITE....51
5.2.7.1 Introduction....51
5.2.7.2 Mobile-originating case....51
5.2.7.3 Mobile-terminating case....51
5.2.7.4 Access network charging information....52
5.2.8 Call release....52
5.2.8.1 P-CSCF-initiated call release....52
5.2.8.1.1 Cancellation of a session currently being established....52
5.2.8.1.2 Release of an existing session....52
5.2.8.1.3 Abnormal cases....53
5.2.8.1.4 Release of the existing dialogs due to registration expiration and deletion of the security association....53
5.2.8.2 Call release initiated by any other entity....53
5.2.8.3 Session expiration....53
5.2.9 Subsequent requests....53
5.2.9.1 Mobile-originating case....53
5.2.9.2 Mobile-terminating case....53
5.2.10 Emergency service....53
5.2.11 Void....54
5.3 Procedures at the I-CSCF....54
5.3.1 Registration procedure....54
5.3.1.1 General....54
5.3.1.2 Normal procedures....54
5.3.1.3 Abnormal cases....55
5.3.2 Initial requests....55
5.3.2.1 Normal procedures....55
5.3.2.2 Abnormal cases....57
5.3.3 THIG functionality in the I-CSCF(THIG)....58
5.3.3.1 General....58
5.3.3.2 Encryption for topology hiding....58
5.3.3.3 Decryption for Topology Hiding....59
5.3.4 Void....59
5.4 Procedures at the S-CSCF....59
5.4.1 Registration and authentication....59
5.4.1.1 Introduction....59
5.4.1.2 Initial registration and user-initiated reregistration....60
5.4.1.2.1 Unprotected REGISTER....60
5.4.1.2.2 Protected REGISTER....61
5.4.1.2.3 Abnormal cases....63
5.4.1.3 Authentication and reauthentication....64
5.4.1.4 User-initiated deregistration....64
5.4.1.5 Network-initiated deregistration....65
5.4.1.6 Network-initiated reauthentication....66
5.4.1.7 Notification of Application Servers about registration status....67
5.4.2 Subscription and notification....68
5.4.2.1 Subscriptions to S-CSCF events....68
5.4.2.1.1 Subscription to the event providing registration state....68
5.4.2.1.2 Notification about registration state....69
5.4.3 General treatment for all dialogs and standalone transactions excluding requests terminated by the S-CSCF....70

5.4.3.1 Determination of mobile-originated or mobile-terminated case ....70
5.4.3.2 Requests initiated by the served user ....70
5.4.3.3 Requests terminated at the served user....73
5.4.3.4 Original dialog identifier....77
5.4.3.5 Void....77
5.4.4 Call initiation ....77
5.4.4.1 Initial INVITE....77
5.4.4.2 Subsequent requests ....78
5.4.4.2.1 Mobile-originating case....78
5.4.4.2.2 Mobile-terminating case....78
5.4.5 Call release....78
5.4.5.1 S-CSCF-initiated session release ....78
5.4.5.1.1 Cancellation of a session currently being established....78
5.4.5.1.2 Release of an existing session ....78
5.4.5.1.2A Release of the existing dialogs due to registration expiration ....79
5.4.5.1.3 Abnormal cases ....79
5.4.5.2 Session release initiated by any other entity....79
5.4.5.3 Session expiration ....79
5.4.6 Call-related requests ....80
5.4.6.1 ReINVITE....80
5.4.6.1.1 Determination of served user....80
5.4.6.1.2 Mobile-originating case....80
5.4.6.1.3 Mobile-terminating case....80
5.4.7 Void ....80
5.5 Procedures at the MGCF ....80
5.5.1 General....80
5.5.2 Subscription and notification ....80
5.5.3 Call initiation ....81
5.5.3.1 Initial INVITE....81
5.5.3.1.1 Calls originated from circuit-switched networks....81
5.5.3.1.2 Calls terminating in circuit-switched networks ....81
5.5.3.2 Subsequent requests ....82
5.5.3.2.1 Calls originating in circuit-switched networks ....82
5.5.3.2.2 Calls terminating in circuit-switched networks ....82
5.5.4 Call release....82
5.5.4.1 Call release initiated by a circuit-switched network....82
5.5.4.2 IM CN subsystem initiated call release....82
5.5.4.3 MGW-initiated call release ....82
5.5.5 Call-related requests ....82
5.5.5.1 ReINVITE....82
5.5.5.1.1 Calls originating from circuit-switched networks ....82
5.5.5.1.2 Calls terminating in circuit-switched networks ....82
5.5.6 Further initial requests ....83
5.6 Procedures at the BGCF ....83
5.6.1 General....83
5.6.2 Session initiation transaction ....83
5.7 Procedures at the Application Server (AS)....83
5.7.1 Common Application Server (AS) procedures ....83
5.7.1.1 Notification about registration status ....83
5.7.1.2 Extracting charging correlation information ....84
5.7.1.3 Access-Network-Info ....84
5.7.1.4 User identify verification at the AS....85
5.7.1.5 Request authorization....87
5.7.1.6 Event notification throttling ....87
5.7.2 Application Server (AS) acting as terminating UA, or redirect server ....87
5.7.3 Application Server (AS) acting as originating UA ....87
5.7.4 Application Server (AS) acting as a SIP proxy....89
5.7.5 Application Server (AS) performing 3rd party call control ....89
5.7.5.1 General....89
5.7.5.2 Call initiation....90
5.7.5.2.1 Initial INVITE ....90
5.7.5.2.2 Subsequent requests....90

5.7.5.3 Call release ..... 90
5.7.5.4 Call-related requests ..... 90
5.7.5.5 Further initial requests ..... 90
5.7.6 Void ..... 91
5.8 Procedures at the MRFC ..... 91
5.8.1 General ..... 91
5.8.2 Call initiation ..... 91
5.8.2.1 Initial INVITE ..... 91
5.8.2.1.1 MRFC-terminating case ..... 91
5.8.2.1.1.1 Introduction ..... 91
5.8.2.1.2 MRFC-originating case ..... 92
5.8.2.2 Subsequent requests ..... 92
5.8.2.2.1 Tones and announcements ..... 92
5.8.3 Call release ..... 92
5.8.3.1 S-CSCF-initiated call release ..... 92
5.8.3.1.1 Tones and announcements ..... 92
5.8.3.2 MRFC-initiated call release ..... 92
5.8.3.2.1 Tones and announcements ..... 92
5.8.2.2.2 Transcoding ..... 93
5.8.4 Call-related requests ..... 93
5.8.4.1 ReINVITE ..... 93
5.8.4.1.1 MRFC-terminating case ..... 93
5.8.4.1.2 MRFC-originating case ..... 93
5.8.4.2 REFER ..... 93
5.8.4.2.1 MRFC-terminating case ..... 93
5.8.4.2.2 MRFC-originating case ..... 93
5.8.4.2.3 REFER initiating a new session ..... 93
5.8.4.2.4 REFER replacing an existing session ..... 93
5.8.4.3 INFO ..... 93
5.8.5 Further initial requests ..... 94
5.9 IMS-ALG ..... 94
5.9.1 General ..... 94

6 Application usage of SDP ..... 94
6.1 Procedures at the UE ..... 94
6.1.1 General ..... 94
6.1.2 Handling of SDP at the originating UE ..... 95
6.1.3 Handling of SDP at the terminating UE ..... 96
6.2 Procedures at the P-CSCF ..... 96
6.3 Procedures at the S-CSCF ..... 97
6.4 Procedures at the MGCF ..... 97
6.4.1 Calls originating from circuit-switched networks ..... 97
6.4.2 Calls terminating in circuit-switched networks ..... 98
6.5 Procedures at the MRFC ..... 98
6.6 Procedures at the AS ..... 98
6.7 Procedures at the IMS-ALG ..... 98

7 Extensions within the present document ..... 99
7.1 SIP methods defined within the present document ..... 99
7.2 SIP headers defined within the present document ..... 99
7.2.0 General ..... 99
7.2.1 Void ..... 99
7.2.2 Void ..... 99
7.2.3 Void ..... 99
7.2.4 Void ..... 99
7.2.5 Void ..... 99
7.2.6 Void ..... 99
7.2.7 Void ..... 99
7.2.8 Void ..... 99
7.2.9 Void ..... 99
7.2.10 Void ..... 99
7.2A Extensions to SIP headers defined within the present document ..... 99

7.2A.1 Extension to WWW-authenticate header ..... 99
7.2A.1.1 Introduction ..... 99
7.2A.1.2 Syntax ..... 99
7.2A.1.3 Operation ..... 100
7.2A.2 Extension to Authorization header ..... 100
7.2A.2.1 Introduction ..... 100
7.2A.2.2 Syntax ..... 100
7.2A.2.3 Operation ..... 100
7.2A.3 Tokenized-by parameter definition (various headers) ..... 100
7.2A.3.1 Introduction ..... 100
7.2A.3.2 Syntax ..... 100
7.2A.3.3 Operation ..... 101
7.2A.4 P-Access-Network-Info header ..... 101
7.2A.4.1 Introduction ..... 101
7.2A.4.2 Syntax ..... 101
7.2A.4.3 Additional coding rules for P-Access-Network-Info header ..... 101
7.2A.5 P-Charging-Vector header ..... 102
7.2A.5.1 Introduction ..... 102
7.2A.5.2 Syntax ..... 102
7.2A.5.2.1 General ..... 102
7.2A.5.2.2 GPRS as IP-CAN ..... 103
7.2A.5.2.3 I-WLAN as IP-CAN ..... 103
7.2A.5.3 Operation ..... 104
7.2A.6 Orig parameter definition ..... 104
7.2A.6.1 Introduction ..... 104
7.2A.6.2 Syntax ..... 104
7.2A.6.3 Operation ..... 104
7.2A.7 Extension to Security-Client, Security-Server and Security-Verify headers ..... 104
7.2A.7.1 Introduction ..... 104
7.2A.7.2 Syntax ..... 104
7.2A.7.3 Operation ..... 104
7.3 Option-tags defined within the present document ..... 104
7.4 Status-codes defined within the present document ..... 105
7.5 Session description types defined within the present document ..... 105
7.6 3GPP IM CN subsystem XML body, version 1 ..... 105
7.6.1 General ..... 105
7.6.2 Document Type Definition ..... 105
7.6.3 DTD description ..... 105
7.7 SIP timers ..... 106
7.8 IM CN subsystem timers ..... 107

8 SIP compression ..... 107
8.1 SIP compression procedures at the UE ..... 107
8.1.1 SIP compression ..... 107
8.1.2 Compression of SIP requests and responses transmitted to the P-CSCF ..... 107
8.1.3 Decompression of SIP requests and responses received from the P-CSCF ..... 108
8.2 SIP compression procedures at the P-CSCF ..... 108
8.2.1 SIP compression ..... 108
8.2.2 Compression of SIP requests and responses transmitted to the UE ..... 108
8.2.3 Decompression of SIP requests and responses received from the UE ..... 108

9 IP-Connectivity Access Network aspects when connected to the IM CN subsystem ..... 109
9.1 Introduction ..... 109
9.2 Procedures at the UE ..... 109
9.2.1 Connecting to the IP-CAN and P-CSCF discovery ..... 109
9.2.2 Handling of the IP-CAN ..... 109
9.2.3 Special requirements applying to forked responses ..... 109

**Annex A (normative): Profiles of IETF RFCs for 3GPP usage ..... 111**

A.1 Profiles ..... 111
A.1.1 Relationship to other specifications ..... 111
A.1.2 Introduction to methodology within this profile ..... 111

A.1.3 Roles ..... 112

A.2 Profile definition for the Session Initiation Protocol as used in the present document ..... 114
A.2.1 User agent role ..... 114
A.2.1.1 Introduction ..... 114
A.2.1.2 Major capabilities ..... 115
A.2.1.3 PDUs ..... 119
A.2.1.4 PDU parameters ..... 120
A.2.1.4.1 Status-codes ..... 120
A.2.1.4.2 ACK method ..... 122
A.2.1.4.3 BYE method ..... 123
A.2.1.4.4 CANCEL method ..... 128
A.2.1.4.5 COMET method ..... 131
A.2.1.4.6 INFO method ..... 131
A.2.1.4.7 INVITE method ..... 131
A.2.1.4.7A MESSAGE method ..... 139
A.2.1.4.8 NOTIFY method ..... 145
A.2.1.4.9 OPTIONS method ..... 151
A.2.1.4.10 PRACK method ..... 157
A.2.1.4.10A PUBLISH method ..... 163
A.2.1.4.11 REFER method ..... 169
A.2.1.4.12 REGISTER method ..... 174
A.2.1.4.13 SUBSCRIBE method ..... 180
A.2.1.4.14 UPDATE method ..... 186
A.2.2 Proxy role ..... 191
A.2.2.1 Introduction ..... 191
A.2.2.2 Major capabilities ..... 192
A.2.2.3 PDUs ..... 196
A.2.2.4 PDU parameters ..... 197
A.2.2.4.1 Status-codes ..... 197
A.2.2.4.2 ACK method ..... 200
A.2.2.4.3 BYE method ..... 201
A.2.2.4.4 CANCEL method ..... 206
A.2.2.4.5 COMET method ..... 209
A.2.2.4.6 INFO method ..... 209
A.2.2.4.7 INVITE method ..... 209
A.2.2.4.7A MESSAGE method ..... 218
A.2.2.4.8 NOTIFY method ..... 224
A.2.2.4.9 OPTIONS method ..... 230
A.2.2.4.10 PRACK method ..... 236
A.2.2.4.10A PUBLISH method ..... 241
A.2.2.4.11 REFER method ..... 248
A.2.2.4.12 REGISTER method ..... 254
A.2.2.4.13 SUBSCRIBE method ..... 260
A.2.2.4.14 UPDATE method ..... 266

A.3 Profile definition for the Session Description Protocol as used in the present document ..... 271
A.3.1 Introduction ..... 271
A.3.2 User agent role ..... 271
A.3.2.1 Major capabilities ..... 272
A.3.2.2 SDP types ..... 272
A.3.2.3 Void ..... 274
A.3.2.4 Void ..... 274
A.3.3 Proxy role ..... 274
A.3.3.1 Major capabilities ..... 274
A.3.3.2 SDP types ..... 275
A.3.3.3 Void ..... 277
A.3.3.4 Void ..... 277

A.4 Profile definition for other message bodies as used in the present document ..... 277

**Annex B (normative): IP-Connectivity Access Network specific concepts when using GPRS to access IM CN subsystem ..... 278**

B.1 Scope ..... 278
B.2 GPRS aspects when connected to the IM CN subsystem ..... 278
B.2.1 Introduction ..... 278
B.2.2 Procedures at the UE ..... 278
B.2.2.1 PDP context activation and P-CSCF discovery ..... 278
B.2.2.1A Modification of a PDP context used for SIP signalling ..... 279
B.2.2.1B Re-establishment of the PDP context for signalling ..... 280
B.2.2.2 Session management procedures ..... 280
B.2.2.3 Mobility management procedures ..... 280
B.2.2.4 Cell selection and lack of coverage ..... 280
B.2.2.5 PDP contexts for media ..... 280
B.2.2.5.1 General requirements ..... 280
B.2.2.5.1A Activation or modification of PDP contexts for media ..... 280
B.2.2.5.2 Special requirements applying to forked responses ..... 281
B.2.2.5.3 Unsuccessful situations ..... 282
B.3 Application usage of SIP ..... 282
B.3.1 Procedures at the UE ..... 282
B.3.1.1 Void ..... 282
B.4 3GPP specific encoding for SIP header extensions ..... 282
B.4.1 Void ..... 282
**Annex C (normative): UICC and USIM Aspects for access to the IM CN subsystem ..... 283**
C.1 Scope ..... 283
C.2 Derivation of IMS parameters from USIM ..... 283
C.3 ISIM Location in 3GPP Systems ..... 283
**Annex D (normative): IP-Connectivity Access Network specific concepts when using I-WLAN to access IM CN subsystem ..... 284**
D.1 Scope ..... 284
D.2 I-WLAN aspects when connected to the IM CN subsystem ..... 284
D.2.1 Introduction ..... 284
D.2.2 Procedures at the WLAN UE ..... 284
D.2.2.1 I-WLAN tunnel activation and P-CSCF discovery ..... 284
D.2.2.2 I-WLAN tunnel procedures ..... 285
D.2.2.2.1 General requirements ..... 285
D.2.2.2.2 Usage of I-WLAN tunnel for media ..... 285
D.2.2.2.3 Special requirements applying to forked responses ..... 285
**Annex E (informative): Change history ..... 286**
History ..... 305

# Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

# 1 Scope

The present document defines a call control protocol for use in the IP Multimedia (IM) Core Network (CN) subsystem based on the Session Initiation Protocol (SIP), and the associated Session Description Protocol (SDP).

The present document is applicable to:

- the interface between the User Equipment (UE) and the Call Session Control Function (CSCF);
- the interface between the CSCF and any other CSCF;
- the interface between the CSCF and an Application Server (AS);
- the interface between the CSCF and the Media Gateway Control Function (MGCF);
- the interface between the S-CSCF and the Multimedia Resource Function Controller (MRFC)
- the interface between the CSCF and the Breakout Gateway Control Function (BGCF);
- the interface between the BGCF and the MGCF;
- the interface between the BGCF and any other BGCF; and
- the interface between the CSCF and an external Multimedia IP network.

Where possible the present document specifies the requirements for this protocol by reference to specifications produced by the IETF within the scope of SIP and SDP. Where this is not possible, extensions to SIP and SDP are defined within the present document. The document has therefore been structured in order to allow both forms of specification.

As the IM CN subsystem is designed to interwork with different IP-Connectivity Access Networks (IP-CANs), the IP-CAN independent aspects of the IM CN subsystem are described in the main body and annex A of this specification. Aspects for connecting a UE to the IM CN subsystem through specific types of IP-CANs are documented separately in the annexes or in separate documents.

NOTE: The present document covers only the usage of SIP and SDP to communicate with the enitities of the IM CN subsystem. It is possible, and not precluded, to use the capabilities of IP-CAN to allow a terminal containing a SIP UA to communicate with SIP servers or SIP UAs outside the IM CN subsystem, and therefore utilise the services provided by those SIP servers. The usage of SIP and SDP for communicating with SIP servers or SIP UAs outside the IM CN subsystem is outside the scope of the present document.

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.002: "Network architecture".

[3] 3GPP TS 23.003: "Numbering, addressing and identification".

[4] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".

[4A] 3GPP TS 23.107: "Quality of Service (QoS) concept and architecture".

[5] 3GPP TS 23.218: "IP Multimedia (IM) Session Handling; IM call model".

[6] 3GPP TS 23.221: "Architectural requirements".

[7] 3GPP TS 23.228: "IP multimedia subsystem; Stage 2".

[7A] 3GPP TS 23.234: "3GPP system to Wireless Local Area Network (WLAN) interworking; System description".

[8] 3GPP TS 24.008: "Mobile radio interface layer 3 specification; Core Network protocols; Stage 3".

[8A] 3GPP TS 24.141: "Presence service using the IP Multimedia (IM) Core Network (CN) subsystem; Stage 3".

[8B] 3GPP TS 24.147: "Conferencing using the IP Multimedia (IM) Core Network (CN) subsystem; Stage 3".

[8C] 3GPP TS 24.234: "3GPP System to Wireless Local Area Network (WLAN) interworking; User Equipment (UE) to network protocols; Stage 3".

[9] 3GPP TS 25.304: "UE Procedures in Idle Mode and Procedures for Cell Reselection in Connected Mode".

[9A] 3GPP TS 25.331: "Radio Resource Control (RRC); Protocol Specification".

[10] 3GPP TS 26.235: "Packet switched conversational multimedia applications; Default codecs".

[10A] 3GPP TS 27.060: "Mobile Station (MS) supporting Packet Switched Services".

[11] 3GPP TS 29.061: "Interworking between the Public Land Mobile Network (PLMN) supporting Packet Based Services and Packet Data Networks (PDN)".

[11A] 3GPP TS 29.162: "Interworking between the IM CN subsystem and IP networks".

[11B] 3GPP TS 29.163: "Interworking between the IP Multimedia (IM) Core Network (CN) subsystem and Circuit Switched (CS) networks".

[11C] 3GPP TS 29.161: "Interworking between the Public Land Mobile Network (PLMN) supporting Packet Based Services with Wireless Local Access and Packet Data Networks (PDN "

[12] 3GPP TS 29.207: "Policy control over Go interface".

[13] 3GPP TS 29.208: "End to end Quality of Service (QoS) signalling flows".

[13A] 3GPP TS 29.209: "Policy control over Gq interface".

[14] 3GPP TS 29.228: "IP Multimedia (IM) Subsystem Cx and Dx Interfaces; Signalling flows and message contents".

[15] 3GPP TS 29.229: "Cx and Dx Interfaces based on the Diameter protocol, Protocol details".

[16] 3GPP TS 32.240: "Telecommunication management; Charging management; Charging architecture and principles".

[17] 3GPP TS 32.260: "Telecommunication management; Charging management; IP Multimedia Subsystem (IMS) charging".

[18] 3GPP TS 33.102: "3G Security; Security architecture".

[19] 3GPP TS 33.203: "Access security for IP based services".

[19A] 3GPP TS 33.210: "IP Network Layer Security".

[20] 3GPP TS 44.018: "Mobile radio interface layer 3 specification, Radio Resource Control Protocol".

[20A] RFC 2401 (November 1998): "Security Architecture for the Internet Protocol".

[20B] RFC 1594 (March 1994): "FYI on Questions and Answers to Commonly asked "New Internet User" Questions".

[20C] RFC 2403 (November 1998) "The Use of HMAC-MD5-96 within ESP and AH".

[20D] RFC 2404 (November 1998) "The Use of HMAC-SHA-1-96 within ESP and AH".

[20E] RFC 2462 (November 1998): "IPv6 Address Autoconfiguration".

[21] RFC 2617 (June 1999): "HTTP Authentication: Basic and Digest Access Authentication".

[22] RFC 3966 (December 2004): "The tel URI for Telephone Numbers".

[23] RFC 2833 (May 2000): "RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals".

[24] RFC 3761 (April 2004): "The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)".

[25] RFC 2976 (October 2000): "The SIP INFO method".

[25A] RFC 3041 (January 2001): "Privacy Extensions for Stateless Address Autoconfiguration in IPv6".

[26] RFC 3261 (June 2002): "SIP: Session Initiation Protocol".

[27] RFC 3262 (June 2002): "Reliability of provisional responses in Session Initiation Protocol (SIP)".

[27A] RFC 3263 (June 2002): " Session Initiation Protocol (SIP): Locating SIP Servers".

[27B] RFC 3264 (June 2002): "An Offer/Answer Model with Session Description Protocol (SDP)".

[28] RFC 3265 (June 2002): "Session Initiation Protocol (SIP) Specific Event Notification".

[29] RFC 3311 (September 2002): "The Session Initiation Protocol (SIP) UPDATE method".

[30] RFC 3312 (October 2002): "Integration of resource management and Session Initiation Protocol (SIP)".

[31] RFC 3313 (January 2003): "Private Session Initiation Protocol (SIP) Extensions for Media Authorization".

[32] RFC 3320 (March 2002): "Signaling Compression (SigComp)".

[33] RFC 3323 (November 2002): "A Privacy Mechanism for the Session Initiation Protocol (SIP)".

[34] RFC 3325 (November 2002): "Private Extensions to the Session Initiation Protocol (SIP) for Network Asserted Identity within Trusted Networks".

[34A] RFC 3326 (December 2002): "The Reason Header Field for the Session Initiation Protocol (SIP)".

[35] RFC 3327 (December 2002): "Session Initiation Protocol Extension Header Field for Registering Non-Adjacent Contacts".

[36] RFC 3515 (April 2003): "The Session Initiation Protocol (SIP) REFER method".

[37] RFC 3420 (November 2002): "Internet Media Type message/sipfrag".

[38] RFC 3608 (October 2003): "Session Initiation Protocol (SIP) Extension Header Field for Service Route Discovery During Registration".

[39] draft-ietf-mmusic-sdp-new-26 (January 2006): "SDP: Session Description Protocol".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[40] RFC 3315 (July 2003): "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)".

[41] RFC 3319 (July 2003): "Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers".

[42] RFC 3485 (February 2003): "The Session Initiation Protocol (SIP) and Session Description Protocol (SDP) static dictionary for Signaling Compression (SigComp)".

[43] RFC 3680 (March 2004): "A Session Initiation Protocol (SIP) Event Package for Registrations".

[44] Void.

[45] Void.

[46] Void.

[47] Void.

[48] RFC 3329 (January 2003): "Security Mechanism Agreement for the Session Initiation Protocol (SIP)".

[49] RFC 3310 (September 2002): "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)".

[50] RFC 3428 (December 2002): "Session Initiation Protocol (SIP) Extension for Instant Messaging".

[51] Void.

[52] RFC 3455 (January 2003): "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)".

[53] RFC 3388 (December 2002): "Grouping of Media Lines in Session Description Protocol".

[54] RFC 3524 (April 2003): "Mapping of Media Streams to Resource Reservation Flows".

[55] RFC 3486 (February 2003): "Compressing the Session Initiation Protocol (SIP)".

[56] RFC 3556 (July 2003): "Session Description Protocol (SDP) Bandwidth Modifiers for RTP Control Protocol (RTCP) Bandwidth".

[56A] RFC 3581 (August 2003): "An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing".

[56B] RFC 3841 (August 2004): "Caller Preferences for the Session Initiation Protocol (SIP)"

[56C] RFC 3646 (December 2003): "DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)".

[57] ITU-T Recommendation E.164: "The international public telecommunication numbering plan".

[58] RFC 4028 ( April 2005): "Session Timers in the Session Initiation Protocol (SIP)".

[59] RFC 3892 (September 2004): "The Session Initiation Protocol (SIP) Referred-By Mechanism".

[60] RFC 3891 (September 2004): "The Session Inititation Protocol (SIP) "Replaces" Header".

[61] RFC 3911 (October 2004): "The Session Inititation Protocol (SIP) "Join" Header".

[62] RFC 3840 (August 2004): "Indicating User Agent Capabilities in the Session Initiation Protocol (SIP)"

[63] RFC 3861 (August 2004): "Address Resolution for Instant Messaging and Presence".

[64] RFC 4032 (March 2005): "Update to the Session Initiation Protocol (SIP) Preconditions Framework".

[70] RFC 3903 (October 2004): "An Event State Publication Extension to the Session Initiation Protocol (SIP)".

[71] Void.

[72] RFC 3857 (August 2004): "A Watcher Information Event Template Package for the Session Initiation Protocol (SIP)".

[74] RFC 3856 (August 2004): "A Presence Event Package for the Session Initiation Protocol (SIP)".

[75] draft-ietf-simple-event-list-07 (December 2004): "A Session Initiation Protocol (SIP) Event Notification Extension for Resource Lists".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[77] draft-ietf-sipping-config-framework-07 (July 2005): "A Framework for Session Initiation Protocol User Agent Profile Delivery".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[78] draft-ietf-sipping-conference-package-12 (July 2005): "A Session Initiation Protocol (SIP) Event Package for Conference State"

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[79] draft-ietf-rohc-sigcomp-sip-01 (February 2004): "Applying Signaling Compression (SigComp) to the Session Initiation Protocol (SIP)".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[85] 3GPP2 C.S0005-D (March 2004), "Upper Layer (Layer 3) Signaling Standard for cdma2000 Standards for Spread Spectrum Systems".

[86] 3GPP2 C.S0024-A v1.0 (April 2004), "cdma2000 High Rate Packet Data Air Interface Standard".

# 3 Definitions and abbreviations

## 3.1 Definitions

For the purposes of the present document, the following terms and definitions apply.

**Newly established set of security associations**: Two pairs of IPsec security associations that have been created at the UE and/or the P-CSCF after the 200 (OK) response to a REGISTER request was received.

**Old set of security associations:** Two pairs of IPsec security associations still in existence after another set of security associations has been established due to a successful authentication procedure.

**Temporary set of security associations:** Two pairs of IPsec security associations that have been created at the UE and/or the P-CSCF, after an authentication challenge within a 401 (Unauthorized) response to a REGISTER request was received. The SIP level lifetime of such created security associations will be equal to the value of reg-await-auth timer.

**Integrity protected:** See 3GPP TS 33.203 [19]. Where a requirement exists to send information "integrity protected" the mechanisms specified in 3GPP TS 33.203 [19] are used for sending the information. Where a requirements exists to check that information was received "integrity protected", then the information received is checked for compliance with the procedures as specified in 3GPP TS 33.203 [19].

**Resource reservation:** Mechanism for reserving bearer resources that is required for certain access technologies.

**Local preconditions:** The indication of segmented status preconditions for the local reservation of resources as specified in RFC 3312 [30].

**Alias SIP URI:** A URI is an alias of another URI if the treatment of both URIs is identical, i.e. both URIs belong to the same set of implicitly registered public user identities, have the same service profile, and both are either shared or not shared.

For the purposes of the present document, the following terms and definitions given in RFC 1594 [20B].

**Fully-Qualified Domain Name (FQDN)**

For the purposes of the present document, the following terms and definitions given in RFC 3261 [26] apply (unless otherwise specified see clause 6).

**Back-to-Back User Agent (B2BUA)**
**Client**
**Dialog**
**Final response**
**Header**
**Header field**
**Loose routeing**
**Method**
**Option-tag** (see RFC 3261 [26] subclause 19.2)
**Provisional response**
**Proxy, proxy server**
**Redirect server**
**Registrar**
**Request**
**Response**
**Server**
**Session**
**(SIP) transaction**
**Stateful proxy**
**Stateless proxy**
**Status-code** (see RFC 3261 [26] subclause 7.2)
**Tag** (see RFC 3261 [26] subclause 19.3)
**Target Refresh Request**
**User agent client (UAC)**
**User agent server (UAS)**
**User agent (UA)**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.002 [2] subclause 4.1.1.1 and subclause 4a.7 apply:

**Breakout Gateway Control Function (BGCF)**
**Call Session Control Function (CSCF)**
**Home Subscriber Server (HSS)**
**Media Gateway Control Function (MGCF)**
**Multimedia Resource Function Controller (MRFC)**
**Multimedia Resource Function Processor (MRFP)**
**Subscription Locator Function (SLF)**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.218 [5] subclause 3.1 apply:

**Filter criteria**
**Initial filter criteria**
**Initial request**
**Standalone transaction**
**Subsequent request**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.228 [7] subclauses 3.1, 4.3.3.1, 4.3.6, 4.6 and 5.4.12.1 apply:

**Interrogating-CSCF (I-CSCF)**
**IMS Application Level Gateway (IMS-ALG)**
**IP-Connectivity Access Network (IP-CAN)**
**Policy Decision Function (PDF)**
**Private user identity**
**Proxy-CSCF (P-CSCF)**
**Public Service Identity (PSI)**
**Public user identity**
**Serving-CSCF (S-CSCF)**
**Statically pre-configured PSI**

For the purposes of the present document, the following terms and definitions given in 3GPP TR 33.203 [19] apply:

**IM Subscriber Identity Module (ISIM)**
**Protected server port**
**Protected client port**

For the purposes of the present document, the following terms and definitions given in 3GPP TR 21.905 [1] apply:

**Universal Integrated Circuit Card (UICC)**
**Universal Subscriber Identity Module (USIM)**
**User Equipment (UE)**

For the purposes of the present document, the following terms and definitions given in RFC 2401 [20A] Appendix A apply:

**Security association**

A number of different security associations exist within the IM CN subsystem and within the underlying access transport. Within this document this term specifically applies to either:

(i) the security association that exists between the UE and the P-CSCF. This is the only security association that has direct impact on SIP. or

(ii) the security association that exists between the WLAN UE and the PDG. This is the security association that is relevant to the discussion of Interworking WLAN as the underlying IP-CAN.

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.002 [1B] apply:

**WLAN UE**
**3GPP AAA proxy**
**3GPP AAA server**
**Packet Data Gateway (PDG)**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.234 [7A] apply.

**Interworking WLAN**

For the purposes of the present document, the following terms and definitions given in ITU-T E.164 [57] apply:

**International public telecommunication number**

## 3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

| | |
|---|---|
| 1xx | A status-code in the range 101 through 199, and excluding 100 |
| 2xx | A status-code in the range 200 through 299 |
| AAA | Authentication, Authorization and Accounting |
| AS | Application Server |
| APN | Access Point Name |
| AUTN | Authentication TokeN |
| B2BUA | Back-to-Back User Agent |
| BGCF | Breakout Gateway Control Function |
| c | conditional |
| CCF | Charging Collection Function |
| CDF | Charging Data Function |
| CDR | Charging Data Record |
| CK | Ciphering Key |
| CN | Core Network |
| CSCF | Call Session Control Function |
| DHCP | Dynamic Host Configuration Protocol |
| DNS | Domain Name System |
| DTD | Document Type Definition |
| ECF | Event Charging Function |

| | |
|---|---|
| FQDN | Fully Qualified Domain Name |
| GCID | GPRS Charging Identifier |
| GGSN | Gateway GPRS Support Node |
| GPRS | General Packet Radio Service |
| HSS | Home Subscriber Server |
| i | irrelevant |
| I-CSCF | Interrogating CSCF |
| ICID | IM CN subsystem Charging Identifier |
| IK | Integrity Key |
| IM | IP Multimedia |
| IMS | IP Multimedia core network Subsystem |
| IMS-ALG | IMS Application Level Gateway |
| IMSI | International Mobile Subscriber Identity |
| IOI | Inter Operator Identifier |
| IP | Internet Protocol |
| IP-CAN | IP-Connectivity Access Network |
| IPsec | IP security |
| IPv4 | Internet Protocol version 4 |
| IPv6 | Internet Protocol version 6 |
| ISC | IP Multimedia Subsystem Service Control |
| ISIM | IM Subscriber Identity Module |
| I-WLAN | Interworking – WLAN |
| m | mandatory |
| MAC | Message Authentication Code |
| MCC | Mobile Country Code |
| MGCF | Media Gateway Control Function |
| MGW | Media Gateway |
| MNC | Mobile Network Code |
| MRFC | Multimedia Resource Function Controller |
| MRFP | Multimedia Resource Function Processor |
| PDG | Packet Data Gateway |
| PDP | Packet Data Protocol |
| PLMN | Public Land Mobile Network |
| PSTN | Public Switched Telephone Network |
| n/a | not applicable |
| NAI | Netework Access Identifier |
| o | optional |
| OCF | Online Charging Function |
| P-CSCF | Proxy CSCF |
| PDU | Protocol Data Unit |
| PSI | Public Service Identity |
| QoS | Quality of Service |
| RAND | RANDom challenge |
| RES | RESponse |
| RTCP | Real-time Transport Control Protocol |
| RTP | Real-time Transport Protocol |
| S-CSCF | Serving CSCF |
| SDP | Session Description Protocol |
| SIP | Session Initiation Protocol |
| SLF | Subscription Locator Function |
| SQN | SeQuence Number |
| UA | User Agent |
| UAC | User Agent Client |
| UAS | User Agent Server |
| UE | User Equipment |
| UICC | Universal Integrated Circuit Card |
| URI | Uniform Resource Identifier |
| URL | Uniform Resource Locator |
| UDVM | Universal Decompressor Virtual Machine |
| USIM | Universal Subscriber Identity Module |
| WLAN | Wireless Local Area Network |
| x | prohibited |

XMAC expected MAC
XML eXtensible Markup Language

# 3A Interoperability with different IP-CAN

The IM CN subsystem can be accessed by UEs resident in different types of IP-CAN. The main body of this document, and annex A, are general to UEs and IM CN subsystems that are accessed using any type of IP-CAN. Requirements that are dependent on the type of IP-CAN are covered in annexes B and D, or in separate specifications.

# 4 General

## 4.1 Conformance of IM CN subsystem entities to SIP, SDP and other protocols

SIP defines a number of roles which entities can implement in order to support capabilities. These roles are defined in annex A.

Each IM CN subsytem functional entity using an interface at the Gm reference point, the Ma reference point, the Mg reference point, the Mi reference point, the Mj reference point, the Mk reference point, the Mm reference point, the Mr reference point and the Mw reference point, and also using the IP multimedia Subsystem Service Control (ISC) Interface, shall implement SIP, as defined by the referenced specifications in Annex A, and in accordance with the constraints and provisions specified in annex A, according to the following roles.

The Gm reference point, the Ma reference point, the Mg reference point, the Mi reference point, the Mj reference point, the Mk reference point, the Mm reference point, the Mr reference point, the Mw reference point and the ISC reference point are defined in 3GPP TS 23.002 [2].

- The User Equipment (UE) shall provide the User Agent (UA) role, with the exceptions and additional capabilities to SIP as described in subclause 5.1, with the exceptions and additional capabilities to SDP as described in subclause 6.1, and with the exceptions and additional capabilities to SigComp as described in subclause 8.1. The UE shall also provide the access dependent procedures described in subclause B.2.2.

- The P-CSCF shall provide the proxy role, with the exceptions and additional capabilities to SIP as described in subclause 5.2, with the exceptions and additional capabilities to SDP as described in subclause 6.2, and with the exceptions and additional capabilities to SigComp as described in subclause 8.2. Under certain circumstances as described in subclause 5.2, the P-CSCF shall provide the UA role with the additional capabilities, as follows:

  a) when acting as a subscriber to or the recipient of event information; and

  b) when performing P-CSCF initiated dialog-release the P-CSCF shall provide the UA role, even when acting as a proxy for the remainder of the dialog.

- The I-CSCF shall provide the proxy role, with the exceptions and additional capabilities as described in subclause 5.3.

- The S-CSCF shall provide the proxy role, with the exceptions and additional capabilities as described in subclause 5.4, and with the exceptions and additional capabilities to SDP as described in subclause 6.3. Under certain circumstances as described in subclause 5.4, the S-CSCF shall provide the UA role with the additional capabilities, as follows:

  a) the S-CSCF shall also act as a registrar. When acting as a registrar, or for the purposes of executing a third-party registration, the S-CSCF shall provide the UA role;

  b) as the notifier of event information the S-CSCF shall provide the UA role;

  c) when providing a messaging mechanism by sending the MESSAGE method, the S-CSCF shall provide the UA role; and

d) when performing S-CSCF initiated dialog release the S-CSCF shall provide the UA role, even when acting as a proxy for the remainder of the dialog.

- The MGCF shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.5, and with the exceptions and additional capabilities to SDP as described in subclause 6.4.

- The BGCF shall provided the proxy role, with the exceptions and additional capabilities as described in subclause 5.6.

- The AS, acting as terminating UA, or redirect server (as defined in 3GPP TS 23.218 [5] subclause 9.1.1.1), shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.7.2, and with the exceptions and additional capabilities to SDP as described in subclause 6.6.

- The AS, acting as originating UA (as defined in 3GPP TS 23.218 [5] subclause 9.1.1.2), shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.7.3, and with the exceptions and additional capabilities to SDP as described in subclause 6.6.

- The AS, acting as a SIP proxy (as defined in 3GPP TS 23.218 [5] subclause 9.1.1.3), shall provided the proxy role, with the exceptions and additional capabilities as described in subclause 5.7.4.

- The AS, performing 3rd party call control (as defined in 3GPP TS 23.218 [5] subclause 9.1.1.4), shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.7.5, and with the exceptions and additional capabilities to SDP as described in subclause 6.6.

NOTE 1: Subclause 5.7 and its subclauses define only the requirements on the AS that relate to SIP. Other requirements are defined in 3GPP TS 23.218 [5].

- The AS, receiving third-party registration requests, shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.7.

- The MRFC shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.8, and with the exceptions and additional capabilities to SDP as described in subclause 6.5.

- The IMS-ALG shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.9, and with the exceptions and additional capabilities to SDP as described in subclause 6.5.

In addition to the roles specified above, the P-CSCF, the I-CSCF, the S-CSCF, the BGCF can act as a UA when providing server functionality to return a final response for any of the reasons specified in RFC 3261 [26].

NOTE 2: Annex A can change the status of requirements in referenced specifications. Particular attention is drawn to table A.4 and table A.162 for capabilities within referenced SIP specifications, and to table A.317 and table A.328 for capabilities within referenced SDP specifications. The remaining tables build on these initial tables.

NOTE 3: The allocated roles defined in this clause are the starting point of the requirements from the IETF SIP specifications, and are then the basis for the description of further requirements. Some of these extra requirements formally change the proxy role into a B2BUA. In all other respects other than those more completely described in subclause 5.2a P-CSCF implements proxy requirements. Despite being a B2BUA a P-CSCF does not implement UA requirements from the IETF RFCs, except as indicated in this specification, e.g., relating to registration event subscription.

## 4.2 URI and address assignments

In order for SIP and SDP to operate, the following preconditions apply:

1) I-CSCFs used in registration are allocated SIP URIs. Other IM CN subsystem entities may be allocated SIP URIs. For example sip:pcscf.home1.net and sip:<impl-specific-info>@pcscf.home1.net are valid SIP URIs. If the user part exists, it is an essential part of the address and shall not be omitted when copying or moving the address. How these addresses are assigned to the logical entities is up to the network operator. For example, a single SIP URI may be assigned to all I-CSCFs, and the load shared between various physical boxes by underlying IP capabilities, or separate SIP URIs may be assigned to each I-CSCF, and the load shared between various physical boxes using DNS SRV capabilities.

2) All IM CN subsystem entities are allocated IPv6 addresses in accordance with the constraints specified in 3GPP TS 23.221 [6] subclause 5.1.

3) The subscriber is allocated a private user identity by the home network operator, and this is contained within the ISIM application, if present. Where no ISIM application is present but USIM is present, the private user identity is derived (see subclause 5.1.1.1A). This private user identity is available to the SIP application within the UE.

NOTE: The SIP URIs may be resolved by using any of public DNSs, private DNSs, or peer-to-peer agreements.

4) The subscriber is allocated one or more public user identities by the home network operator. The public user identity shall take the form of SIP URI as specified in RFC 3261 [26] or tel URI as specified in RFC 3966 [22]. At least one of these is SIP URI and it is contained within the ISIM application, if ISIM application is present. Where no ISIM application is present but USIM is present, the UE derives a temporary public user identity (see subclause 5.1.1.1A). All registered public user identities are available to the SIP application within the UE, after registration.

5) For each tel URI, there is at least one alias SIP URI in the set of implicitly registered public user identities that is used to implicitly register the associated tel URI.

6) The public user identities may be shared across multiple UEs. A particular public user identity may be simultaneously registered from multiple UEs that use different private user identities and different contact addresses. When reregistering and deregistering a given public user identity and associated contact address, the UE will use the same private user identity that it has used during the initial registration of the respective public user identity and associated contact address.If the tel URI is a shared public user identity, then the associated alias SIP URI is also a shared public user identity. Likewise, if the alias SIP URI is a shared public user identity, then the associated tel URI is also a shared public user identity.

7) For the purpose of access to the IM CN subsystem, UEs are assigned IPv6 prefixes in accordance with the constraints specified in 3GPP TS 23.221 [6] subclause 5.1 (see subclause 9.2.1 for the assignment procedures).

## 4.2A Transport mechanisms

This document makes no requirement on the transport protocol used to transfer signalling information over and above that specified in RFC 3261 [26] clause 18. However, the UE and IM CN subsystem entities shall transport SIP messages longer than 1300 bytes according to the procedures of RFC 3261 [26] subclause 18.1.1, even if a mechanism exists of discovering a maximum transmission unit size longer than 1500 bytes.

For initial REGISTER requests, the UE and the P-CSCF shall apply port handling according to subclause 5.1.1.2 and subclause 5.2.2.

The UE and the P-CSCF shall send and receive request and responses other then initial REGISTER requests on the protected ports as described in 3GPP TS 33.203 [19].

## 4.3 Routeing principles of IM CN subsystem entities

Each IM CN subsytem functional entity shall apply loose routeing policy as described in RFC 3261 [26], when processing a SIP request. In cases where the I-CSCF or the S-CSCFmay interact with strict routers in non IM CN subsystem networks, the routeing procedures defined in RFC 3261 [26] that ensure interoperability with strict routers shall be used by the I-CSCF and S-CSCF.

## 4.4 Trust domain

RFC 3325 [34] provides for the existence and trust of an asserted identity within a trust domain. For the IM CN subsystem, this trust domain consists of the functional entities that belong to the same operator's domain (P-CSCF, the I-CSCF, the S-CSCF, the BGCF. the MGCF, the MRFC, and all ASs that are not provided by third-party service providers). Additionally, other IMS nodes that are not part of the same operator's domain may or may not be part of the trust domain, depending on whether an interconnect agreement exists with the remote network. SIP functional entities that belong to a network for which there is an interconnect agreement are part of the trust domain. ASs provided by third-party service providers are outside the trust domain. SIP functional entities within the trust domain will need to take an action on the removal of the P-Asserted-Identity header when SIP signalling crosses the boundary of the trust domain.

Editor's Note: the exact mechanism to determine which nodes are part of the trust domain and which nodes are not, is FFS.

For the purpose of the P-Access-Network-Info header, a trust domain also applies. This trust domain is identical to that of the P-Asserted-Identity. For the P-Access-Network-Info header, subclause 5.4 also identifies additional cases for the removal of the header.

NOTE: In addition to the procedures specified in clause 5, procedures of RFC 3325 [34] in relation to transmission of P-Asserted-Identity headers and their contents outside the trust domain also apply.

# 4.5 Charging correlation principles for IM CN subsystems

## 4.5.1 Overview

This subclause describes charging correlation principles to aid with the readability of charging related procedures in clause 5. See 3GPP TS 32.240 [16] and 3GPP TS 32.260 [17] for further information on charging.

The IM CN subsystem generates and retrieves the following charging correlation information for later use with offline and online charging:

1. IM CN subsystem Charging Identifier (ICID);
2. Access network charging information;
3. Inter Operator Identifier (IOI);
4. Charging function addresses:
   a. Charging Data Function (CDF);
   b. Online Charging Function (OCF).

How to use and where to generate the parameters in IM CN subsystems are described further in the subclauses that follow. The charging correlation information is encoded in the P-Charging-Vector header as defined in subclause 7.2A.5. The P-Charging-Vector header contains the following parameters: icid, access network charging information and ioi.

The offline and online charging function addresses are encoded in the P-Charging-Function-Addresses as defined in RFC 3455 [52]. The P-Charging-Function-Addresses header contains the following parameters: "ccf" for CDF and "ecf" for OCF.

NOTE: P-Charging-Function-Addresses parameters were defined using previous terminology.

## 4.5.2 IM CN subsystem charging identifier (ICID)

The ICID is the session level data shared among the IM CN subsystem entities including ASs in both the calling and called IM CN subsystems. The ICID is used also for session unrelated messages (e.g. SUBSCRIBE request, NOTIFY request, MESSAGE request) for the correlation with CDRs generated among the IM CN subsystem entities.

The first IM CN subsystem entity involved in a SIP transaction will generate the ICID and include it in the icid parameter of the P-Charging-Vector header in the SIP request. For a dialog relating to a session, this will be performed only on the INVITE request, for all other transactions, it will occur on each SIP request. See 3GPP TS 32.260 [17] for requirements on the format of ICID. The P-CSCF will generate an ICID for mobile-originated calls. The I-CSCF will generate an ICID for mobile-terminated calls if there is no ICID received in the initial request (e.g. the calling party network does not behave as an IM CN subsystem). The AS will generate an ICID when acting as an originating UA. The MGCF will generate an ICID for PSTN/PLMN originated calls. Each entity that processes the SIP request will extract the ICID for possible later use in a CDR. The I-CSCF and S-CSCF are also allowed to generate a new ICID for mobile terminated calls received from another network.

There is also an ICID generated by the P-CSCF with a REGISTER request that is passed in a unique instance of P-Charging-Vector header. The valid duration of the ICIDis specified in 3GPP TS 32.260 [17].

The icid parameter is included in any requests that include the P-Charging-Vector header. However, the P-Charging-Vector (and ICID) is not passed to the UE.

The ICID is also passed from the P-CSCF to the IP-CAN via PDF. The interface supporting this operation is outside the scope of this document.

## 4.5.3 Access network charging information

### 4.5.3.1 General

The access network charging information are the media flow level data shared among the IM CN subsystem entities for one side of the session (either the calling or called side). GPRS charging information (GGSN identifier and PDP context information) is an example of access network charging information.

### 4.5.3.2 Access network charging information

The IP-CAN provides the access network charging information to the IM CN subsystem. This information is used to correlate IP-CAN CDRs with IM CN subsystem CDRs, i.e. the access network charging information is used to correlate the bearer level with the session level.

The access network charging information is generated at the first opportunity after the resources are allocated at the IP-CAN. The access network charging information is passed from IP-CAN to P-CSCF via PDF, over the Go and Gq interfaces. Access network charging information will be updated with new information during the session as media flows are added or removed. The P-CSCF provides the access network charging information to the S-CSCF. The S-CSCF may also pass the information to an AS, which may be needed for online pre-pay applications. The access network charging information for the originating network is used only within that network, and similarly the access network charging information for the terminating network is used only within that network. Thus the access network charging information are not shared between the calling and called networks. The access network charging information is not passed towards the external ASs from its own network.

The access network charging information is populated in the P-Charging-Vector header.

## 4.5.4 Inter operator identifier (IOI)

The Inter Operator Identifier (IOI) is a globally unique identifier to share between sending and receiving networks, service providers or content providers.

The sending network populates the orig-ioi parameter of the P-Charging-Vector header in a request and thereby identifies the operator network from which the request originated. The term-ioi parameter is left out of the P-Charging-Vector header in this request. The sending network retrieves the term-ioi parameter from the P-Charging-Vector header within the message sent in response, which identifies the operator network from which the response was sent.

The receiving network retrieves the orig-ioi parameter from the P-Charging-Vector header in the request, which identifies the operator network from which the request originated. The receiving network populates the term-ioi parameter of the P-Charging-Vector header in the response to the request, which identifies the operator network from which the response was sent.

There are three types of IOI:

- Type 1 IOI, between the P-CSCF (possibly in the visited network) and the S-CSCF in the home network. This is exchanged in REGISTER requests and responses.

- Type 2 IOI, between the S-CSCF of the home originating network and the S-CSCF of the home terminating network or between the S-CSCF of the home originating network and the MGCF when a call/session is terminated at the PSTN/PLMN or between the MGCF and the S-CSCF of the home terminating network when a call/session is originated from the PSTN/PLMN or with a PSI AS when accessed accross I-CSCF. This is exchanged in all session-related and session-unrelated requests and responses. The Type 2 IOI will not be passed along within the network, except when proxied by BGCF and I-CSCF to get to MGCF and S-CSCF. For compatibility issues related to CS charging system behaviour simulation, the S-CSCF in the terminating network shall forward the orig-ioi parameter from the P-Charging-Vector header in the initial request, which identifies the operator network from which the request originated.

Editor's Note: The solution documented above results in overloading of the IOI parameter to the AS add additional complexity to the billing system in identifying the required IOI pair, some investigation is still in progress to see if a simpler solution can be adopted that meets the requirements.

- Type 3 IOI, between the S-CSCF of the home operator network and any AS. This is exchanged in all session-related and session-unrelated requests and responses.

IOIs will not be passed along within the network, except when proxied by BGCF and I-CSCF to get to MGCF and S-CSCF. However, IOIs will be sent to the AS for accounting purposes.

Each entity that processes the SIP request will extract the IOI for possible later use in a CDR. The valid duration of the IOI is specified in 3GPP TS 32.240 [16].

### 4.5.5 Charging function addresses

Charging function addresses are distributed to each of the IM CN subsystem entities in the home network for one side of the session (either the calling or called side) and are to provide a common location for each entity to send charging information. Charging Data Function (CDF) addresses are used for offline billing. Online Charging Function (OCF) addresses are used for online billing.

There may be multiple addresses for CDF and OCF addresses populated into the P-Charging-Function-Addresses header of the SIP request or response. The parameters are ccf and ecf for CDF and OCF, respectively. At least one instance of either ccf or ecf is required. If ccf address is included for offline charging, then a secondary ccf address may be included by each network for redundancy purposes, but the first instance of ccf is the primary address. If ecf address is included for online charging, then a secondary instance may also be included for redundancy.

The CDF and/or OCF addresses are retrieved from an Home Subscriber Server (HSS) via the Cx interface and passed by the S-CSCF to subsequent entities. The charging function addresses are passed from the S-CSCF to the IM CN subsystem entities in its home network, but are not passed to the visited network or the UE. When the P-CSCF is allocated in the visited network, then the charging function addresses are obtained by means outside the scope of this document. The AS receives the charging function addresses from the S-CSCF via the ISC interface. CDF and/or OCF addresses may be allocated as locally preconfigured addresses. The AS may also retrieve the charging function address from the HSS via Sh interface.

# 5 Application usage of SIP

## 5.1 Procedures at the UE

### 5.1.1 Registration and authentication

#### 5.1.1.1 General

The UE shall register public user identities (see table A.4/1 and dependencies on that major capability).

In case a UE registers several public user identities at different points in time, the procedures to re-register, deregister and subscribe to the registration-state event package for these public user identities can remain uncoordinated in time.

#### 5.1.1.1A Parameters contained in the ISIM

The ISIM application shall always be used for IMS authentication, if it is present, as described in 3GPP TS 33.203 [19].

The ISIM is preconfigured with all the necessary parameters to initiate the registration to the IM CN subsystem. These parameters include:

- the private user identity;
- one ore more public user identities; and
- the home network domain name used to address the SIP REGISTER request

In case the UE is loaded with a UICC that does not contain the ISIM application, the UE shall:

- generate a private user identity;
- generate a temporary public user identity; and
- generate a home network domain name to address the SIP REGISTER request to;

in accordance with the procedures in clause C.2.

The temporary public user identity is only used in REGISTER requests, i.e. initial registration, re-registration, mobile-initiated deregistration. After a successful registration, the UE will get the associated public user identities, and the UE may use any of them in subsequent non-REGISTER requests.

The UE shall not reveal to the user the temporary public user identity if the temporary public user identity is barred. The temporary public user identity is not barred if received by the UE in the P-Associated-URI header.

If the UE is unable to derive the parameters in this subclause for any reason, then the UE shall not proceed with the request associated with the use of these parameters and will not be able to register to the IM CN subsystem.

#### 5.1.1.2 Initial registration

The UE can register a public user identity with its contact address at any time after it has aquired an IP address, discovered a P-CSCF, and established an IP-CAN bearer that can be used for SIP signalling. However, the UE shall only initiate a new registration procedure when it has received a final response from the registrar for the ongoing registration, or the previous REGISTER request has timed out.

The UE shall send only the initial REGISTER requests to the port advertised to the UE during the P-CSCF discovery procedure. If the UE does not receive any specific port information during the P-CSCF discovery procedure, the UE shall send the initial REGISTER request to the SIP default port values as specified in RFC 3261 [26].

The UE shall extract or derive a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration, according to the procedures described in subclause 5.1.1.1A. A public user identity may be input by the end user.

On sending a REGISTER request, the UE shall populate the header fields as follows:

a) an Authorization header, with:
   - the username directive, set to the value of the private user identity;
   - the realm directive, set to the domain name of the home network;
   - the uri directive, set to the SIP URI of the domain name of the home network;
   - the nonce directive, set to an empty value; and
   - the response directive, set to an empty value;

b) a From header set to the SIP URI that contains the public user identity to be registered;

c) a To header set to the SIP URI that contains the public user identity to be registered;

d) a Contact header set to include SIP URI(s) containing the IP address of the UE in the hostport parameter or FQDN. If the REGISTER request is protected by a security association, the UE shall also include the protected server port value in the hostport parameter;

e) a Via header set to include the IP address or FQDN of the UE in the sent-by field. If the REGISTER request is protected by a security association, the UE shall also include the protected server port value in the sent-by field

NOTE 1: If the UE specifies its FQDN in the host parameter in the Contact header and in the sent-by field in the Via header, then it has to ensure that the given FQDN will resolve (e.g., by reverse DNS lookup) to the IP address that is bound to the security association.

NOTE 2: The UE associates two ports, a protected client port and a protected server port, with each pair of security association. For details on the selection of the protected port value see 3GPP TS 33.203 [19].

f) an Expires header, or the expires parameter within the Contact header, set to the value of 600 000 seconds as the value desired for the duration of the registration;

NOTE 3: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 (Interval Too Brief) response.

g) a Request-URI set to the SIP URI of the domain name of the home network;

h) the Security-Client header field set to specify the security mechanism the UE supports, the IPsec layer algorithms the UE supports and the parameters needed for the security association setup. The UE shall support the setup of two pairs of security associations as defined in 3GPP TS 33.203 [19]. The syntax of the parameters needed for the security association setup is specified in Annex H of 3GPP TS 33.203 [19]. The UE shall support the "ipsec-3gpp" security mechanism, as specified in RFC 3329 [48]. The UE shall support the HMAC-MD5-96 (RFC 2403 [20C]) and HMAC-SHA-1-96 (RFC 2404 [20D]) IPsec layer algorithms, and shall announce support for them according to the procedures defined in RFC 3329 [48];

i) the Supported header containing the option tag "path"; and

j) if a security association exists, a P-Access-Network-Info header set as specified for the access network technology (see subclause 7.2A.4).

On receiving the 200 (OK) response to the REGISTER request, the UE shall:

a) store the expiration time of the registration for the public user identities found in the To header value;

b) store the list of URIs contained in the P-Associated-URI header value. This list contains the URIs that are associated to the registered public user identity;

c) store as the default public user identity the first URI on the list of URIs present in the P-Associated-URI header;

d) treat the identity under registration as a barred public user identity, if it is not included in the P-Associated-URI header;

e) store the list of Service-Route headers contained in the Service-Route header, in order to build a proper preloaded Route header value for new dialogs and standalone transactions; and

f) set the security association lifetime to the longest of either the previously existing security association lifetime (if available), or the lifetime of the just completed registration plus 30 seconds.

When a 401 (Unauthorized) response to a REGISTER is received the UE shall behave as described in subclause 5.1.1.5.1.

On receiving a 305 (Use Proxy) response to the initial REGISTER request, the UE shall:

a) release all IP-CAN bearers used for the transport of media according to the procedures in subclause 9.2.2;

b) initiate a new P-CSCF discovery procedure as described in subclause 9.2.1;

c) select a P-CSCF address, which is different from the previously used address, from the address list; and

d) perform the procedures for initial registration as described in subclause 5.1.1.2.

On receiving a 423 (Interval Too Brief) too brief response to the REGISTER request, the UE shall:

- send another REGISTER request populating the Expires header or the expires parameter with an expiration timer of at least the value received in the Min-Expires header of the 423 (Interval Too Brief) response.

### 5.1.1.3 Initial subscription to the registration-state event package

Upon receipt of a 2xx response to the initial registration, the UE shall subscribe to the reg event package for the public user identity registered at the user's registrar (S-CSCF) as described in RFC 3680 [43].

The UE shall use the default public user identiy for subscription to the registration-state event package, if the public user identity that was used for initial registration is a barred public user identity. The UE may use either the default

public user identity or the public user identity used for initial registration for the subscription to the registration-state event package, if the initial public user identity that was used for initial registration is not barred.

On sending a SUBSCRIBE request, the UE shall populate the header fields as follows:

a) a Request URI set to the resource to which the UE wants to be subscribed to, i.e. to a SIP URI that contains the public user identity used for subscription;

b) a From header set to a SIP URI that contains the public user identity used for subscription;

c) a To header set to a SIP URI that contains the public user identity used for subscription;

d) an Event header set to the "reg" event package;

e) an Expires header set to 600 000 seconds as the value desired for the duration of the subscription

f) a P-Access-Network-Info header set as specified for the access network technology (see subclause 7.2A.4); and

g) a Contact header set to contain the same IP address or FQDN, and with the protected server port value as in the initial registration.

Upon receipt of a 2xx response to the SUBSCRIBE request, the UE shall store the information for the established dialog and the expiration time as indicated in the Expires header of the received response.

If continued subscription is required, the UE shall automatically refresh the subscription by the reg event package, for a previously registered public user identity, either 600 seconds before the expiration time if the initial subscription was for greater than 1200 seconds, or when half of the time has expired if the initial subscription was for 1200 seconds or less.

#### 5.1.1.4 User-initiated re-registration

The UE can reregister a previously registered public user identity with its contact address at any time.

Unless either the user or the application within the UE has determined that a continued registration is not required the UE shall reregister the public user identity either 600 seconds before the expiration time if the initial registration was for greater than 1200 seconds, or when half of the time has expired if the initial registration was for 1200 seconds or less, or when the UE intends to update its capabilities according to RFC 3840 [62].

The UE shall protect the REGISTER request using a security association, see 3GPP TS 33.203 [19], established as a result of an earlier registration, if IK is available.

The UE shall extract or derive a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration, according to the procedures described in subclause 5.1.1.1A.

On sending a REGISTER request that does not contain a challenge response, the UE shall populate the header fields as follows:

a) an Authorization header, with:

- the username directive set to the value of the private user identity;
- the realm directive, set to the domain name of the home network;
- the uri directive, set to the SIP URI of the domain name of the home network;
- the nonce directive, set to last received nonce value; and
- the response directive, set to the last calculated response value;

b) a From header set to the SIP URI that contains the public user identity to be registered;

c) a To header set to the SIP URI that contains the public user identity to be registered;

d) a Contact header set to include SIP URI(s) that contain(s) in the hostport parameter the IP address of the UE or FQDN and protected server port value bound to the security association;

e) a Via header set to include the IP address or FQDN of the UE in the sent-by field and the protected server port value bound to the security association;

NOTE 1: If the UE specifies its FQDN in the host parameter in the Contact header and in the sent-by field in the Via header, then it has to ensure that the given FQDN will resolve (e.g., by reverse DNS lookup) to the IP address that is bound to the security association.

NOTE 2: The UE associates two ports, a protected client port and a protected server port, with each pair of security associations. For details on the selection of the protected port value see 3GPP TS 33.203 [19].

f) an Expires header, or an expires parameter within the Contact header, set to 600 000 seconds as the value desired for the duration of the registration;

NOTE 3: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 (Interval Too Brief) response.

g) a Request-URI set to the SIP URI of the domain name of the home network;

h) a Security-Client header field, set to specify the security mechanism it supports, the IPsec layer algorithms it supports and the new parameter values needed for the setup of two new pairs of security associations. For further details see 3GPP TS 33.203 [19] and RFC 3329 [48];

i) a Security-Verify header that contains the content of the Security-Server header received in the 401 (Unauthorized) response of the last successful authentication;

j) the Supported header containing the option tag "path"; and

k) the P-Access-Network-Info header set as specified for the access network technology (see subclause 7.2A.4).

On receiving the 200 (OK) response to the REGISTER request, the UE shall:

a) store the new expiration time of the registration for this public user identity found in the To header value;

b) store the list of URIs contained in the P-Associated-URI header value. This list contains the URIs that are associated to the registered public user identity;

c) store the list of Service-Route headers contained in the Service-Route header, in order to build a proper preloaded Route header value for new dialogs and standalone transactions; and

d) set the security association lifetime to the longest of either the previously existing security association lifetime, or the lifetime of the just completed registration plus 30 seconds.

When a 401 (Unauthorized) response to a REGISTER is received the UE shall behave as described in subclause 5.1.1.5.1.

On receiving a 423 (Interval Too Brief) response to the REGISTER request, the UE shall:

- send another REGISTER request populating the Expires header or the expires parameter with an expiration timer of at least the value received in the Min-Expires header of the 423 (Interval Too Brief) response.

On receiving a 408 (Request Timeout) response or 500 (Server Internal Error) response or 504 (Server Time-Out) response for a reregistration, the UE shall perform the procedures for initial registration as described in subclause 5.1.1.2.

On receiving a 305 (Use Proxy) response to the REGISTER request, the UE shall:

a) release all IP-CAN bearers used for the transport of media according to the procedures in subclause 9.2.2;

b) initiate a new P-CSCF discovery procedure as described in subclause 9.2.1;

c) select a P-CSCF address, which is different from the previously used address, from the address list; and

d) perform the procedures for initial registration as described in subclause 5.1.1.2.

When the timer F expires at the UE, the UE shall:

1) stop processing of all ongoing dialogs and transactions and silently discard them locally; and

2) after releasing all IP-CAN bearers used for the transport of media according to the procedures in subclause 9.2.2, the UE may:

   a) select a different P-CSCF address from the list of P-CSCF addresses discovered during the procedures described in subclause 9.2.1;

   b) if no response has been received when attempting to contact all P-CSCFs known by the UE, the UE may get a new set of P-CSCF-addresses as described in subclause 9.2.1; and

   c) perform the procedures for initial registration as described in subclause 5.1.1.2.

NOTE 4: It is an implementation option whether these actions are also triggered by other means than expiration of timer F, e.g. based on ICMP messages.

After a maximum of 5 consecutive initial registration attempts, the UE shall not automatically attempt any further initial registration for an implementation dependant time of at least 30 minutes.

### 5.1.1.5 Authentication

#### 5.1.1.5.1 General

Authentication is achieved via the registration and re-registration procedures. When the network requires authentication or re-authentication of the UE, the UE will receive a 401 (Unauthorized) response to the REGISTER request.

On receiving a 401 (Unauthorized) response to the REGISTER request, the UE shall:

1) extract the RAND and AUTN parameters;

2) check the validity of a received authentication challenge, as described in 3GPP TS 33.203 [19] i.e. the locally calculated XMAC must match the MAC parameter derived from the AUTN part of the challenge; and the SQN parameter derived from the AUTN part of the challenge must be within the correct range; and

3) check the existence of the Security-Server header as described in RFC 3329 [48]. If the header is not present or it does not contain the parameters required for the setup of the set of security associations (see annex H of 3GPP TS 33.203 [19]), the UE shall abandon the authentication procedure and send a new REGISTER request with a new Call-ID.

In the case that the 401 (Unauthorized) response to the REGISTER request is deemed to be valid the UE shall:

1) calculate the RES parameter and derive the keys CK and IK from RAND as described in 3GPP TS 33.203 [19];

2) set up a temporary set of security associations based on the static list and parameters it received in the 401 (Unauthorized) response and its capabilities sent in the Security-Client header in the REGISTER request. The UE sets up the temporary set of security associations using the most preferred mechanism and algorithm returned by the P-CSCF and supported by the UE and using IK as the shared key. The UE shall use the parameters received in the Security-Server header to setup the temporary set of security associations. The UE shall set a temporary SIP level lifetime for the temporary set of security associations to the value of reg-await-auth timer; and

3) send another REGISTER request using the temporary set of security associations to protect the message. The header fields are populated as defined for the initial request, with the addition that the UE shall include an Authorization header containing the private user identity and the authentication challenge response calculated by the UE using RES and other parameters, as described in RFC 3310 [49]. The UE shall also insert the Security-Client header that is identical to the Security-Client header that was included in the previous REGISTER request (i.e. the REGISTER request that was challenged with the received 401 (Unauthorized) response). The UE shall also insert the Security-Verify header into the request, by mirroring in it the content of the Security-Server header received in the 401 (Unauthorized) response. The UE shall set the Call-ID of the integrity protected REGISTER request which carries the authentication challenge response to the same value as the Call-ID of the 401 (Unauthorized) response which carried the challenge.

On receiving the 200 (OK) response for the integrity protected REGISTER request, the UE shall:

- change the temporary set of security associations to a newly established set of security associations, i.e. set its SIP level lifetime to the longest of either the previously existing set of security associations SIP level lifetime, or the lifetime of the just completed registration plus 30 seconds;and

- use the newly established set of security associations for further messages sent towards the P-CSCF as appropriate.

NOTE 1: In this case, the UE will send requests towards the P-CSCF over the newly established set of security associations. Responses towards the P-CSCF that are sent via UDP will be sent over the newly established set of security associations. Responses towards the P-CSCF that are sent via TCP will be sent over the same set of security associations that the related request was received on.

When the first request or response protected with the newly established set of security associations is received from the P-CSCF, the UE shall delete the old set of security associations and related keys it may have with the P-CSCF after all SIP transactions that use the old set of security associations are completed.

Whenever the 200 (OK) response is not received before the temporary SIP level lifetime of the temporary set of security associations expires or a 403 (Forbidden) response is received, the UE shall consider the registration to have failed. The UE shall delete the temporary set of security associations it was trying to establish, and use the old set of security associations. The UE should send an unprotected REGISTER message according to the procedure specified in subclause 5.1.1.2 if the UE considers the old set of security associations to be no longer active at the P-CSCF.

In the case that the 401 (Unauthorized) response is deemed to be invalid then the UE shall behave as defined in subclause 5.1.1.5.3.

#### 5.1.1.5.2 Network-initiated re-authentication

At any time, the UE can receive a NOTIFY request carrying information related to the reg event package (as described in subclause 5.1.1.3). If:

- the state attribute in any of the <registration> elements is set to "active";

- the value of the <uri> sub-element inside the <contact> sub-element is set to the Contact address that the UE registered; and

- the event attribute of that <contact> sub-element(s) is set to "shortened";

the UE shall:

1) use the expiry attribute within the <contact> sub-element that the UE registered to adjust the expiration time for that public user identity; and

2) start the re-authentication procedures at the appropriate time (as a result of the S-CSCF procedure described in subclause 5.4.1.6) by initiating a reregistration as described in subclause 5.1.1.4, if required.

NOTE: When authenticating a given private user identity, the S-CSCF will only shorten the expiry time within the <contact> sub-element that the UE registered using its private user identity. The <contact> elements for the same public user identitity, if registered by another UE using different private user identities remain unchanged. The UE will not initiate a reregistration procedure, if none of its <contact> sub-elements was modified.

#### 5.1.1.5.3 Abnormal cases

If, in a 401 (Unauthorized) response, either the MAC or SQN is incorrect the UE shall respond with a further REGISTER indicating to the S-CSCF that the challenge has been deemed invalid as follows:

- in the case where the UE deems the MAC parameter to be invalid the subsequent REGISTER request shall contain no AUTS directive and an empty response directive, i.e. no authentication challenge response;

- in the case where the UE deems the SQN to be out of range, the subsequent REGISTER request shall contain the AUTS directive (see 3GPP TS 33.102 [18]).

NOTE: In the case of the SQN being out of range, a response directive can be included by the UE, based on the procedures described in RFC 3310 [49].

Whenever the UE detects any of the above cases, the UE shall:

- send the REGISTER request using an existing set of security associations, if available (see 3GPP TS 33.203 [19]);
- populate a new Security-Client header within the REGISTER request, set to specify the security mechanism it supports, the IPsec layer algorithms it supports and the parameters needed for the new security association setup; and
- not create a temporary set of security associations.

A UE shall only respond to two consecutive invalid challenges. The UE may attempt to register with the network again after an implementation specific time.

### 5.1.1.5A Change of Ipv6 address due to privacy

Stateless address autoconfiguration as described in RFC 2462 [20E] defines how an IPv6 prefix and an interface identifier is used by the UE to construct a complete IPv6 address.

If the UE receives an IPv6 prefix, the UE may change the interface identity of the IPv6 address as described in RFC 3041 [25A] due to privacy but this will result in service discontinuity for IMS services.

NOTE: The procedure described below will terminate all established dialogs and transactions and temporarily disconnect the UE from the IM CN subsystem until the new registration is performed. Due to this, the UE is recommended to provide a limited use of the procedure to ensure a maximum degree of continuous service to the end user.

In order to change the IPv6 address due to privacy, the UE shall:

1) terminate all ongoing dialogs (e.g., sessions) and transactions (e.g., subscription to the reg event);
2) deregister all registered public user identities as described in subsclause 5.1.1.4;
3) construct a new IPv6 address according to the procedures specified in RFC 3041 [25A];
4) register the public user identities that were deregistered in step 2 above, as follows:
   a) by performing an initial registration as described in subsclause 5.1.1.2; and
   b) by performing a subscription to the reg event package as described in subsclause 5.1.1.3; and
5) subscribe to other event packages it was subscribed to before the change of IPv6 address procedure started.

### 5.1.1.6 User-initiated deregistration

The UE can deregister a public user identity that it has previously registered with its contact address at any time.

The UE shall integrity protect the REGISTER request using a security association, see 3GPP TS 33.203 [19], established as a result of an earlier registration, if one is available.

The UE shall extract or derive a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration, according to the procedures described in subclause 5.1.1.1A.

Prior to sending a REGISTER request for deregistration, the UE shall release all dialogs related to the public user identity that is going to be deregistered or to one of the implicitly registered public user identities.

On sending a REGISTER request, the UE shall populate the header fields as follows:

a) an Authorization header, with:
   - the username directive, set to the value of the private user identity;
   - the realm directive, set to the domain name of the home network;
   - the uri directive, set to the SIP URI of the domain name of the home network;

- the nonce directive, set to last received nonce value; and
- the response directive, set to the last calculated response value;

b) a From header set to the SIP URI that contains the public user identity to be deregistered;

c) a To header set to the SIP URI that contains the public user identity to be deregistered;

d) a Contact header set to either the value of "*" or SIP URI(s) that contain(s) in the hostport parameter the IP address of the UE or FQDN and the protected server port value bound to the security association;

e) a Via header set to include the IP address or FQDN of the UE in the sent-by field and the protected server port value bound to the security association;

NOTE 1: If the UE specifies its FQDN in the host parameter in the Contact header and in the sent-by field in the Via header, then it has to ensure that the given FQDN will resolve (e.g., by reverse DNS lookup) to the IP address that is bound to the security association.

f) an Expires header, or the expires parameter of the Contact header, set to the value of zero, appropriate to the deregistration requirements of the user;

g) a Request-URI set to the SIP URI of the domain name of the home network; and

h) a P-Access-Network-Info header set as specified for the access network technology (see subclause 7.2A.4).

On receiving the 200 (OK) response to the REGISTER request, the UE shall remove all registration details relating to this public user identity.

If there are no more public user identities registered, the UE shall delete the security associations and related keys it may have towards the IM CN subsystem.

If all public user identities are deregistered and the security association is removed, then the UE shall consider subscription to the reg event package cancelled (i.e. as if the UE had sent a SUBSCRIBE request with an Expires header containing a value of zero).

NOTE: When the UE has received the 200 (OK) response for the REGISTER request of the only public user identity currently registered with its associated set of implicitly registered public user identities (i.e. no other is registered), the UE removes the security association established between the P-CSCF and the UE. Therefore further SIP signalling (e.g. the NOTIFY request containing the deregistration event) will not reach the UE.

#### 5.1.1.7 Network-initiated deregistration

Upon receipt of a NOTIFY request on the dialog which was generated during subscription to the reg event package as described in subclause 5.1.1.3, including one or more <registration> element(s) which were registered by this UE with:

- the state attribute set to "terminated" and the event attribute set to "rejected" or "deactivated"; or
- the state attribute set to "active" and the state attribute within the <contact> element belonging to this UE set to "terminated", and associated event attribute element to "rejected" or "deactivated";

the UE shall remove all registration details relating to these public user identities. In case of a "deactivated" event attribute, the UE shall start the initial registration procedure as described in subclause 5.1.1.2. In case of a "rejected" event attribute, the UE shall release all dialogs related to those public user identities.

Upon receipt of a NOTIFY request, the UE shall delete the security associations towards the P-CSCF either:

- if all <registration> element(s) having their state attribute set to "terminated" (i.e. all public user identities are deregistered) and the Subscription-State header contains the value of "terminated"; or
- if each <registration> element that was registered by this UE has either the state attribute set to "terminated", or the state attribute set to "active" and the state attribute within the <contact> element belonging to this UE set to "terminated".

The UE shall delete these security associations towards the P-CSCF after the server transaction (as defined in RFC 3261 [26]) pertaining to the received NOTIFY request terminates.

NOTE 1: Deleting a security association is an internal procedure of the UE and does not involve any SIP procedures.

NOTE 2: If all the public user identities or contact addresses registered by this UE are deregistered and the security association is removed, then the UE considers the subscription to the reg event package terminated (i.e. as if the UE had sent a SUBSCRIBE request with an Expires header containing a value of zero, or a NOTIFY request was received with Subscription-State header containing the value of "terminated").

NOTE 3: When the P-CSCF has removed the security association established between the P-CSCF and the UE, further SIP signalling (e.g. the NOTIFY containing the deregistration event) will not reach the UE.

## 5.1.2 Subscription and notification

### 5.1.2.1 Notification about multiple registered public user identities

Upon receipt of a 2xx response to the SUBSCRIBE request the UE shall maintain the generated dialog (identified by the values of the Call-ID, To and From headers).

Upon receipt of a NOTIFY request on the dialog which was generated during subscription to the reg event package the UE shall perform the following actions:

- if a state attribute "active", i.e. registered is received for one or more public user identities, the UE shall store the indicated public user identities as registered;

- if a state attribute "terminated", i.e. deregistered is received for one or more public user identities, the UE shall store the indicated public user identities as deregistered.

NOTE: There may be public user identities which are automatically registered within the registrar (S-CSCF) of the user upon registration of one public user identity. Usually these automatically or implicitly registered public user identities belong to the same service profile of the user and they might not be available within the UE. The implicitly registered public user identities may also belong to different service profiles. The here-described procedures provide a different mechanism (to the 200 (OK) response to the REGISTER request) to inform the UE about these automatically registered public user identities.

### 5.1.2.2 General SUBSCRIBE requirements

If the UA receives a 503 (Service Unavailable) response to an initial SUBSCRIBE request containing a Retry-After header, then the UE shall not automatically reattempt the request until after the period indicated by the Retry-After header contents.

## 5.1.2A Generic procedures applicable to all methods excluding the REGISTER method

### 5.1.2A.1 Mobile-originating case

The procedures of this subclause are general to all requests and responses, except those for the REGISTER method.

When the UE sends any request, the UE shall:

- include the protected server port in the Via header entry relating to the UE; and

- include the protected server port in any Contact header that is otherwise included.

The UE shall discard any SIP response that is not integrity protected and is received from the P-CSCF outside of the registration and authentication procedures. The requirements on the UE within the registration and authentication procedures are defined in subclause 5.1.1.

In accordance with RFC 3325 [34] the UE may insert a P-Preferred-Identity header in any initial request for a dialog or request for a standalone transaction as a hint for creation of an asserted identity within the IM CN subsystem. The UE may include any of the following in the P-Preferred-Identity header:

- a public user identity which has been registered by the user;

- a public user identity returned in a registration-state event package of a NOTIFY request as a result of an implict registration that was not subsequently deregistered or has expired; or

- any other public user identity which the user has assumed by mechanisms outside the scope of this specification to have a current registration.

NOTE 1: The temporary public user identity specified in subclause 5.1.1.1 is not a public user identity suitable for use in the P-Preferred-Identity header.

NOTE 2: Procedures in the network require international public telecommunication numbers when telephone numbers are used in P-Preferred-Identity header.

NOTE 3: A number of headers can reveal information about the identity of the user. Where privacy is required, implementers should also give consideration to other headers that can reveal identity information. RFC 3323 [33] subclause 4.1 gives considerations relating to a number of headers.

Where privacy is required, in any initial request for a dialog or request for a standalone transaction, the UE shall set the From header to "Anonymous".

NOTE 4: The contents of the From header should not be relied upon to be modified by the network based on any privacy specified by the user either within the UE indication of privacy or by network subscription or network policy. Therefore the user should include the value "Anonymous" whenever privacy is explicitly required. As the user may well have privacy requirements, terminal manufacturers should not automatically derive and include values in this header from the public user identity or other values stored in or derived from the UICC. Where the user has not expressed a preference in the configuration of the terminal implementation, the implementation should assume that privacy is required. Users that require to identify themselves, and are making calls to SIP destinations beyond the IM CN subsystem, where the destination does not implement RFC 3325 [34], will need to include a value in the From header other than Anonymous.

The UE can indicate privacy of the P-Asserted-Identity that will be generated by the P-CSCF in accordance with RFC 3323 [33], and the additional requirements contained within RFC 3325 [34].

The UE shall insert a P-Access-Network-Info header into any request for a dialog, any subsequent request (except ACK requests and CANCEL requests) or response (except CANCEL responses) within a dialog or any request for a standalone method. The UE shall populate the P-Access-Network-Info header with the current point of attachment to the IP-CAN as specified for the access network technology (see subclause 7.2A.4).

NOTE 5: During the dialog, the points of attachment to the IP-CAN of the UE may change (e.g. UE connects to different cells). The UE will populate the P-Access-Network-Info header in any request or response within a dialog with the current point of attachment to the IP-CAN (e.g. the current cell information).

The UE shall build a proper preloaded Route header value for all new dialogs and standalone transactions. The UE shall build a list of Route header values made out of, in this order, the P-CSCF URI (containing the IP address or the FQDN learnt through the P-CSCF discovery procedures, and the protected server port learnt during the registration procedure), and the values received in the Service-Route header saved from the 200 (OK) response to the last registration or re-registration.

When a SIP transaction times out, i.e. timer B, timer F or timer H expires at the UE, the UE may behave as if timer F expired, as described in subclause 5.1.1.4.

NOTE 6: It is an implementation option whether these actions are also triggered by other means.

### 5.1.2A.2 Mobile-terminating case

The procedures of this subclause are general to all requests and responses, except those for the REGISTER method.

When the UE sends any response, the UE shall:

- include the protected server port in any Contact header that is otherwise included.

The UE shall discard any SIP request that is not integrity protected and is received from the P-CSCF outside of the registration and authentication procedures. The requirements on the UE within the registration and authentication procedures are defined in subclause 5.1.1.

The UE can indicate privacy of the P-Asserted-Identity that will be generated by the P-CSCF in accordance with RFC 3323 [33], and the additional requirements contained within RFC 3325 [34].

NOTE 1: In the mobile-terminating case, this version of the document makes no provision for the UE to provide an P-Preferred-Identity in the form of a hint.

NOTE 2: A number of headers can reveal information about the identity of the user. Where, privacy is required, implementers should also give consideration to other headers that can reveal identity information. RFC 3323 [33] subclause 4.1 gives considerations relating to a number of headers.

The UE shall insert a P-Access-Network-Info header into any response to a request for a dialog, any subsequent request (except CANCEL requests) or response (except CANCEL responses) within a dialog or any response to a standalone method. The UE shall populate the P-Access-Network-Info header with its current point of attachment to the IP-CAN as specified for the access network technology (see subclause 7.2A.4).

## 5.1.3 Call initiation - mobile originating case

### 5.1.3.1 Initial INVITE request

The "integration of resource management and SIP" extension is hereafter in this subclause referred to as "the precondition mechanism" and is defined in RFC 3312 [30] as updated by RFC 4032 [64].

The precondition mechanism should be supported by the originating UE.

The UE may initiate a session without the precondition mechanism if the originating UE does not require local resource reservation.

NOTE 1: The originating UE can decide if local resource reservation is required based on e.g. application requirements, current access network capabilities, local configuration, etc.

In order to allow the peer entity to reserve its required resources, an originating UE supporting the precondition mechanism should make use of the precondition mechanism, even if it does not require local resource reservation.

Upon generating an initial INVITE request using the precondition mechanism, the UE shall:

- indicate the support for reliable provisional responses and specify it using the Supported header mechanism; and
- indicate the support for the preconditions mechanism and specify it using the Supported header mechanism.

Upon generating an initial INVITE request using the precondition mechanism, the UE should not indicate the requirement for the precondition mechanism by using the Require header mechanism.

NOTE 2: If an UE chooses to require the precondition mechanism, i.e. if it indicates the "precondition" option tag within the Require header, the interworking with a remote UE, that does not support the precondition mechanism, is not described in this specification.

The UE may indicate that proxies should not fork the INVITE request by including a "no-fork" directive within the Request-Disposition header in the initial INVITE request as described in RFC 3841 [56B].

NOTE 3: Table A.4 specifies that UE support of forking is required in accordance with RFC 3261 [26]. The UE can accept or reject any of the forked responses, for example, if the UE is capable of supporting a limited number of simultaneous transactions or early dialogs.

Upon successful reservation of local resources the UE shall confirm the successful resource reservation (see subclause 6.1.2) within the next SIP request.

NOTE 4: In case of the precondition mechanism being used on both sides, this confirmation will be sent in either a PRACK request or an UPDATE request. In case of the precondition mechanism not being supported on one or both sides, alternatively a reINVITE request can be used for this confirmation, in case the terminating UE does not support the PRACK request (as described in RFC 3262 [27]) and does not support the UPDATE request (as described in RFC 3311 [29]).

When a final answer is received for one of the early dialogues, the UE proceeds to set up the SIP session. The UE shall not progress any remaining early dialogues to established dialogs. Therefore, upon the reception of a subsequent final 200 (OK) response for an INVITE request (e.g., due to forking), the UE shall:

1) acknowledge the response with an ACK request; and

2) send a BYE request to this dialog in order to terminate it.

Upon receiving a 488 (Not Acceptable Here) response to an initial INVITE request, the originating UE should send a new INVITE request containing SDP according to the procedures defined in subclause 6.1.

NOTE 5: An example of where a new request would not be sent is where knowledge exists within the UE, or interaction occurs with the user, such that it is known that the resulting SDP would describe a session that did not meet the user requirements.

Upon receiving a 421 (Extension Required) response to an initial INVITE request in which the precondition mechanism was not used, including the "precondition" option tag in the Require header, the originating UE shall send a new INVITE request using the precondition mechanism, if the originating UE supports the precondition mechanism.

Upon receiving a 503 (Service Unavailable) response to an initial INVITE request containing a Retry-After header, then the originating UE shall not automatically reattempt the request until after the period indicated by the Retry-After header contents.

## 5.1.4 Call initiation - mobile terminating case

### 5.1.4.1 Initial INVITE request

The precondition mechanism should be supported by the terminating UE.

The handling of incoming initial INVITE requests at the terminating UE is mainly dependent on the following conditions:

- the specific service requirements for "integration of resource management and SIP" extension (hereafter in this subclause known as the precondition mechanism and defined in RFC 3312 [30] as updated by RFC 4032 [64], and with the request for such a mechanism known as a precondition); and

- the UEs configuration for the case when the specific service does not require the precondition mechanism.

Editor's Note: The detailed criteria when to use the non-precondition procedures / resource reservation should be either derived from stage 2 or should be included as a reference to 3GPP TS 23.228.

If an initial INVITE request is received the terminating UE shall check whether the terminating UE requires local resource reservation.

NOTE 1: The terminating UE can decide if local resource reservation is required based on e.g. application requirements, current access network capabilities, local configuration, etc.

If local resource reservation is required at the terminating UE and the terminating UE supports the precondition mechanism, and:

a) the received INVITE request includes the "precondition" option-tag in the Supported header or Require header, the terminating UE shall make use of the precondition mechanism and shall indicate a Require header with the "precondition" option-tag in any response or subsequent request it sends towards to the originating UE; or

b) the received INVITE request does not include the "precondition" option-tag in the Supported header or Require header the terminating UE shall not make use of the precondition mechanism.

If local resource reservation is not required by the terminating UE and the terminating UE supports the precondition mechanism and:

a) the received INVITE request includes the "precondition" option-tag in the Supported header and

   - the required resources at the originating UE are not reserved, the terminating UE shall use the precondition mechanism; or

- the required local resources at the originating UE and the terminating UE are available, the terminating UE may use the precondition mechanism;

b) the received INVITE request does not include the "precondition" option-tag in the Supported header or Require header, the terminating UE shall not make use of the precondition mechanism; or

c) the received INVITE request includes the "precondition" option-tag in the Require header, the terminating UE shall use the precondition mechanism.

NOTE 2: Table A.4 specifies that UE support of forking is required in accordance with RFC 3261 [26].

Editor's Note: The above note needs further investigation.

NOTE 3: If the terminating UE does not support the precondition mechanism it will apply regular SIP session initiation procedures.

If the terminating UE requires a reliable alerting indication at the originating side, it shall send the 180 (Ringing) response reliably. The terminating UE shall send provisional responses reliably only if the provisional response carries SDP or for other application related purposes that requires its reliable transport.

### 5.1.5 Call release

Void.

### 5.1.6 Emergency service

A UE shall not attempt to establish an emergency session via the IM CN Subsystem when the UE can detect that the number dialled is an emergency number. The UE shall use the CS domain as described in 3GPP TS 24.008 [8].

In the event the UE receives a 380 (Alternative Service) response to an INVITE request the response containing a XML body that includes an <alternative service> element with the <type> child element set to "emergency", the UE shall automatically:

- send an ACK request to the P-CSCF as per normal SIP procedures;

- attempt an emergency call setup according to the procedures described in 3GPP TS 24.008 [8].

The UE may also provide an indication to the user based on the text string contained in the <reason> element.

As a consequence of this, a UE operating in MS operation mode C cannot perform emergency calls.

### 5.1.7 Void

## 5.2 Procedures at the P-CSCF

### 5.2.1 General

The P-CSCF shall support the Path and Service-Route headers.

NOTE 1: The Path header is only applicable to the REGISTER request and its 200 (OK) response. The Service-Route header is only applicable to the 200 (OK) response of REGISTER request.

When the P-CSCF sends any request or response to the UE, before sending the message the P-CSCF shall:

- remove the P-Charging-Function-Addresses and P-Charging-Vector headers, if present.

When the P-CSCF receives any request or response from the UE, the P-CSCF shall:

- remove the P-Charging-Function-Addresses and P-Charging-Vector headers, if present. Also, the P-CSCF shall ignore any data received in the P-Charging-Function-Addresses and P-Charging-Vector headers; and

- may insert previously saved values into the P-Charging-Function-Addresses and P-Charging-Vector headers before forwarding the message.

NOTE 2: When the P-CSCF is located in the visited network, then it will not receive the P-Charging-Function-Addresses header from the S-CSCF or I-CSCF. Instead, the P-CSCF discovers charging function addresses by other means not specified in this document.

When the P-CSCF receives any request or response containing the P-Media-Authorization header from the S-CSCF, the P-CSCF shall remove the header.

NOTE 3: If service based local policy applies, the P-CSCF will insert the P-Media-Authorization header as described in subclauses 5.2.7.2 and 5.2.7.3.

NOTE 4: The P-CSCF will integrity protect all SIP messages sent to the UE outside of the registration and authentication procedures. The P-CSCF will discard any SIP message that is not integirity protected and is received outside of the registration and authentication procedures. The integrity protection and checking requirements on the P-CSCF within the registration and authentication procedures are defined in subclause 5.2.2.

## 5.2.2 Registration

The P-CSCF shall be prepared to receive only the initial REGISTER requests on the SIP default port values as specified in RFC 3261 [26]. The P-CSCF shall also be prepared to receive the initial REGISTER requests on the port advertised to the UE during the P-CSCF discovery procedure.

When the P-CSCF receives a REGISTER request from the UE, the P-CSCF shall:

1) insert a Path header in the request including an entry containing:

   - the SIP URI identifying the P-CSCF;

   - an indication that requests routed in this direction of the path (i.e. from the S-CSCF to the P-CSCF) are expected to be treated as for the mobile-terminating case. This indication may e.g. be in a parameter in the URI, a character string in the user part of the URI, or be a port number in the URI;

2) insert a Require header containing the option tag "path";

3) insert a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.260 [17] and a type 1 orig-ioi parameter. The P-CSCF shall set the type 1 orig-ioi parameter to a value that identifies the sending network of the request. The P-CSCF shall not include the type 1 term-ioi parameter;

4) insert the parameter "integrity-protected" (described in subclause 7.2A.2) with a value "yes" into the Authorization header field in case the REGISTER request was either received integrity protected with the security association created during an ongoing authentication procedure and includes an authentication challenge response (i.e. RES parameter), or it was received on the security association created during the last successful authentication procedure and with no authentication challenge response (i.e. no RES parameter), otherwise insert the parameter with the value "no";

5) in case the REGISTER request was received without integrity protection, then check the existence of the Security-Client header. If the header is present, then remove and store it. If the header is not present, then the P-CSCF shall return a suitable 4xx response;

6) in case the REGISTER request was received integrity protected, then the P-CSCF shall:

   a) check the security association which protected the request. If the security association is a temporary one, then the request is expected to contain a Security-Verify header in addition to a Security-Client header. If there are no such headers, then the P-CSCF shall return a suitable 4xx response. If there are such headers, then the P-CSCF shall compare the content of the Security-Verify header with the content of the Security-Server header sent earlier and the content of the Security-Client header with the content of the Security-Client header received in the challenged REGISTER. If those do not match, then there is a potential man-in-the-middle attack. The request should be rejected by sending a suitable 4xx response. If the contents match, the P-CSCF shall remove the Security-Verify and the Security-Client header;

   b) if the security association the REGISTER request was received on, is an already established one, then:

- the P-CSCF shall remove the Security-Verify header if it is present;
- a Security-Client header containing new parameter values is expected. If this header or any required parameter is missing, then the P-CSCF shall return a suitable 4xx response;
- the P-CSCF shall remove and store the Security-Client header before forwarding the request to the S-CSCF; and

c) check if the private user identity conveyed in the Authorization header of the integrity-protected REGISTER request is the same as the private user identity which was previously challenged or authenticated. If the private user identities are different, the P-CSCF shall reject the REGISTER request by returning a 403 (Forbidden) response;

7) insert a P-Visited-Network-ID header field, with the value of a pre-provisioned string that identifies the visited network at the home network; and

8) determine the I-CSCF of the home network and forward the request to that I-CSCF.

If the selected I-CSCF:

- does not respond to the REGISTER request and its retransmissions by the P-CSCF; or
- sends back a 3xx response or 480 (Temporarily Unavailable) response to a REGISTER request;

the P-CSCF shall select a new I-CSCF and forward the original REGISTER request.

NOTE 1: The list of the I-CSCFs may be either obtained as specified in RFC 3263 [27A] or provisioned in the P-CSCF.

If the P-CSCF fails to forward the REGISTER request to any I-CSCF, the P-CSCF shall send back a 408 (Request Timeout) response or 504 (Server Time-Out) response to the user, in accordance with the procedures in RFC 3261 [26].

When the P-CSCF receives a 401 (Unauthorized) response to a REGISTER request, the P-CSCF shall:

1) delete any temporary set of security associations established towards the UE;

2) remove the CK and IK values contained in the 401 (Unauthorized) response and bind them to the proper private user identity and to the temporary set of security associations which will be setup as a result of this challenge. The P-CSCF shall forward the 401 (Unauthorized) response to the UE if and only if the CK and IK have been removed;

3) insert a Security-Server header in the response, containing the P-CSCF static security list and the parameters needed for the security association setup, as specified in Annex H of 3GPP TS 33.203 [19]. The P-CSCF shall support the "ipsec-3gpp" security mechanism, as specified in RFC 3329 [48]. The P-CSCF shall support the HMAC-MD5-96 (RFC 2403 [20C]) and HMAC-SHA-1-96 (RFC 2404 [20D]) IPsec layer algorithms;

4) set up the temporary set of security associations with a temporary SIP level lifetime between the UE and the P-CSCF for the user identified with the private user identity. For further details see 3GPP TS 33.203 [19] and RFC 3329 [48]. The P-CSCF shall set the temporary SIP level lifetime for the temporary set of security associations to the value of reg-await-auth timer; and

5) send the 401 (Unauthorized) response to the UE using the security association with which the associated REGISTER request was protected, or unprotected in case the REGISTER request was received unprotected.

NOTE 2: The challenge in the 401 (Unauthorized) response sent back by the S-CSCF to the UE as a response to the REGISTER request is piggybacked by the P-CSCF to insert the Security-Server header field in it. The S-CSCF authenticates the UE, while the P-CSCF negotiates and sets up two pairs of security associations with the UE during the same registration procedure. For further details see 3GPP TS 33.203 [19].

When the P-CSCF receives a 200 (OK) response to a REGISTER request, the P-CSCF shall check the value of the Expires header field and/or Expires parameter in the Contact header. When the value of the Expires header field and/or expires parameter in the Contact header is different than zero, then the P-CSCF shall:

1) save the list of Service-Route headers preserving the order. The P-CSCF shall store this list during the entire registration period of the respective public user identity. The P-CSCF shall use this list to validate the routeing

information in the requests originated by the UE. If this registration is a reregistration, the P-CSCF shall replace the already existing list of Service-Route headers with the new list;

2) associate the Service-Route header list with the registered public user identity;

3) store the public user identities found in the P-Associated-URI header value and associate them to the public user identity under regististation;

4) store the default public user identity for use with procedures for the P-Asserted-Identity header. The default public user identity is the first on the list of URIs present in the P-Associated-URI header;

NOTE 3: There may be more then one default public user identities stored in the P-CSCF, as the result of the multiple registrations of public user identities.

5) store the values received in the P-Charging-Function-Addresses header;

6) if a term-ioi parameter is received in the P-Charging-Vector header, store the value of the received term-ioi parameter;

NOTE 4: Any received term-ioi parameter will be a type 1 term-ioi. The type 1 term-ioi identifies the home network of the registered user.

7) if an existing set of security association is available, set the SIP level lifetime of the security association to the longest of either the previously existing security association lifetime, or the lifetime of the just completed registration plus 30 seconds;

8) if a temporary set of security associations exists, change the temporary set of security associations to a newly established set of security associations, i.e. set its SIP level lifetime to the longest of either the previously existing set of security associations SIP level lifetime, or the lifetime of the just completed registration plus 30 seconds; and

9) protect the 200 (OK) response to the REGISTER request within the same security association to that in which the request was protected.

When receiving a SIP message (including REGISTER requests) from the UE over the newly established set of security associations that have not yet been taken into use, the P-CSCF shall:

1) reduce the SIP level lifetime of the old set of security associations towards the same UE to 64*T1 (if currently longer than 64*T1); and

2) use the newly established set of security associations for further messages sent towards the UE as appropriate (i.e. take the newly established set of security associations into use).

NOTE 5: In this case, the P-CSCF will send requests towards the UE over the newly established set of security associations. Responses towards the UE that are sent via UDP will be sent over the newly established set of security associations. Responses towards the UE that are sent via TCP will be sent over the same set of security associations that the related request was received on.

NOTE 6: When receiving a SIP message (including REGISTER requests) from the UE over a set of security associations that is different from the newly established set of security associations, the P-CSCF will not take any action on any set of security associations.

When the SIP level lifetime of an old set of security associations is about to expire, i.e. their SIP level lifetime is shorther than 64*T1 and a newly established set of security associations has not been taken into use, the P-CSCF shall use the newly estabslihed set of security associations for further messages towards the UE as appropriate (see NOTE 3).

When sending the 200 (OK) response for a REGISTER request that concludes a re-authentication, the P-CSCF shall:

1) keep the set of security associations that was used for the REGISTER request that initiated the re-authentication;

2) keep the newly established set of security associations created during this authentication;

3) delete, if existing, any other set of security associations towards this UE immediately; and

4) go on using for further requests sent towards the UE the set of security associations that was used to protect the REGISTER request that initiated the re-authentication.

When sending the 200 (OK) respone for a REGISTER request that concludes an initial authentication, i.e. the initial REGISTER request was received unprotected, the P-CSCF shall:

1) keep the newly established set of security associations created during this authentication;

2) delete, if existing, any other set of security associations towards this UE immediately; and

3) use the kept newly established set of security associations for further messages sent towards the UE.

NOTE 7: The P-CSCF will maintain two Route header lists. The first Route header list - created during the registration procedure - is used only to validate the routeing information in the initial requests that originate from the UE. This list is valid during the entire registration of the respective public user identity. The second Route list - constructed from the Record Route headers in the initial INVITE and associated response - is used during the duration of the call. Once the call is terminated, the second Route list is discarded.

The P-CSCF shall delete any security association from the IPsec database when their SIP level lifetime expires.

The handling of the security associations at the P-CSCF is summarized in table 5.2.2-1.

**Table 5.2.2-1: Handling of security associations at the P-CSCF**

| | **Temporary set of security associations** | **Newly established set of security associations** | **Old set of security associations** |
|---|---|---|---|
| SIP message received over newly established set of security associations that have not yet been taken into use | No action | Take into use | Reduce SIP level lifetime to 64*T1, if lifetime is larger than 64*T1 |
| SIP message received over old set of security associations | No action | No action | No action |
| Old set of security associations currently in use will expire in 64*T1 | No action | Take into use | No action |
| Sending an authorization challenge within a 401 (Unauthorized) response for a REGISTER request | Create<br>Remove any previously existing temporary set of security associations | No action | No action |
| Sending 200 (OK) response for REGISTER request that concludes re-authentication | Change to a newly established set of security associations | Convert to and treat as old set of security associations (see next column) | Continue using the old set of security associations over which the REGISTER request, that initiated the re-authentication was received. Delete all other old sets of security associations immediately |
| Sending 200 (OK) response for REGISTER request that concludes initial authentication | Change to a newly established set of security associations and take into use immediately | Convert to old set of security associations, i.e. delete | Delete |

## 5.2.3 Subscription to the user's registration-state event package

Upon receipt of a 200 (OK) response to the initial REGISTER request of an user, the P-CSCF shall subscribe to the reg event package at the users registrar (S-CSCF) as described in RFC 3680 [43]. The P-CSCF shall:

1) generate a SUBSCRIBE request with the following elements:

   - a Request-URI set to the resource to which the P-CSCF wants to be subscribed to, i.e. to a SIP URI that contains the default public user identity of the user;

   - a From header set to the P-CSCF's SIP URI;

   - a To header, set to a SIP URI that contains the default public user identity of the user;

- an Event header set to the "reg" event package;
- an Expires header set to a value higher then the Expires header indicated in the 200 (OK) response to the REGISTER request;
- a P-Asserted-Identity header set to the SIP URI of the P-CSCF,which was inserted into the Path header during the registration of the user to whose registration state the P-CSCF subscribes to; and
- a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.260 [17]; and

2) determine the I-CSCF of the home network (e.g., by using DNS services);

before sending the SUBSCRIBE request to that I-CSCF, according to the procedures of RFC 3261 [26].

Upon receipt of a 2xx response to the SUBSCRIBE request, the P-CSCF shall store the information for the so established dialog and the expiration time as indicated in the Expires header of the received response.

If continued subscription is required the P-CSCF shall automatically refresh the subscription by the reg event package 600 seconds before the expiration time for a previously registered public user identity, either 600 seconds before the expiration time if the initial subscription was for greater than 1200 seconds, or when half of the time has expired if the initial subscription was for 1200 seconds or less.

### 5.2.4 Registration of multiple public user identities

Upon receipt of a 2xx response to the SUBSCRIBE request the P-CSCF shall maintain the generated dialog (identified by the values of the Call-ID, To and From headers).

Upon receipt of a NOTIFY request on the dialog which was generated during subscription to the reg event package of the user, the P-CSCF shall perform the following actions:

1) for each public user identity whose state attribute in the <registration> element is set to "active", i.e. registered; and
   - the state attribute within the <contact> sub-element is set to "active"; and
   - the value of the <uri> sub-element inside the <contact> sub-element is set to the contact address of the user's UE; and
   - the event attribute of that <contact> sub-element(s) is set to "registered" or "created";

   the P-CSCF shall:
   - bind the indicated public user identity as registered to the contact information of the respective user;and
   - add the public user identity to the list of the public user identities that are registered for the user;
2) for each public user identity whose state attribute in the <registration> element is set to "active", i.e. registered: and
   - the state attribute within the <contact> sub-element is set to "terminated";
   - the value of the <uri> sub-element inside the <contact> sub-element is set to the contact address of the user's UE; and
   - the event attribute of that <contact> sub-element(s) is set to "deactivated", "expired", "probation", "unregistered", or "rejected";

   the P-CSCF shall consider the indicated public user identitiy as deregistered for this user, and shall release all stored information for the public user identity bound to the respective user; and
3) for each public user identity whose state attribute in the <registration> element is set to "terminated", i.e. deregistered; and
   - the value of the <uri> sub-element inside the <contact> sub-element is set to the contact address of the user's UE; and

- the event attribute of that <contact> sub-element(s) is set to "deactivated", "expired", "probation", "unregistered", or "rejected";

the P-CSCF shall consider the indicated public user identitiy as deregistered for this UE, and shall release all stored information for these public user identity bound to the respective user and remove the public user identity from the list of the public user identities that are registered for the user.

If all public user identities, that were registered by the user using its private user identity, have been deregistered, the P-CSCF, will receive from the S-CSCF a NOTIFY request that may include the Subscription-State header set to "terminated", as described in subclause 5.4.2.1.2. If the Subscription-State header was not set to "terminated", the P-CSCF may either unsubscribe to the reg event package of the user or let the subscription expire.

NOTE 1: Upon receipt of a NOTIFY request with the Subscription-State header set to "terminated", the P-CSCF considers the subscription to the reg event package terminated (i.e. as if the P-CSCF had sent a SUBSCRIBE request with an Expires header containing a value of zero).

NOTE 2: There may be public user identities which are implicitly registered within the registrar (S-CSCF) of the user upon registration of one public user identity. The procedures in this subclause provide a mechanism to inform the P-CSCF about these implicitly registered public user identities.

## 5.2.5 Deregistration

### 5.2.5.1 User-initiated deregistration

When the P-CSCF receives a 200 (OK) response to a REGISTER request (sent according to subclause 5.2.2) sent by this UE, it shall check the value of the Expires header field and/or expires parameter in the Contact header field. When the value of the Expires header field or expires parameter equals zero, then the P-CSCF shall:

1) remove the public user identity found in the To header field, and all the associated public user identities, from the registered public user identities list belonging to this UE and all related stored information; and

2) check if the UE has left any other registered public user identity. When all of the public user identities that were registered by this UE are deregistered, the P-CSCF shall delete the security associations towards the UE, after the server transaction (as defined in RFC 3261 [26]) pertaining to this deregistration terminates.

NOTE 1: Upon receipt of a NOTIFY request with all <registration> element(s) having their state attribute set to "terminated" (i.e. all public user identities are deregistered) and the Subscription-State header set to "terminated", the P-CSCF considers the subscription to the reg event package terminated (i.e. as if the P-CSCF had sent a SUBSCRIBE request with an Expires header containing a value of zero).

NOTE 2: There is no requirement to distinguish a REGISTER request relating to a registration from that relating to a deregistration. For administration reasons the P-CSCF may distinguish such requests, however this has no impact on the SIP procedures.

NOTE 3: When the P-CSCF has sent the 200 (OK) response for the REGISTER request of the only public user identity currently registered with its associated set of implicitly registered public user identities (i.e. no other is registered), the P-CSCF removes the security association established between the P-CSCF and the UE. Therefore further SIP signalling (e.g. the NOTIFY request containing the deregistration event) will not reach the UE.

### 5.2.5.2 Network-initiated deregistration

Upon receipt of a NOTIFY request on the dialog which was generated during subscription to the reg event package of the UE, as described in subclause 5.2.3, including one or more <registration> element(s) which were registered by the UE with either:

- the state attribute set to "terminated"; or

- the state attribute set to "active" and the state attribute within the <contact> sub-element belonging to this UE set to "terminated", and associated event attribute element to "rejected" or "deactivated";

the P-CSCF shall remove all stored information for these public user identities for this UE and remove these public user identities from the list of the public user identities that are registered for the user.

Upon receipt of a NOTIFY request with all <registration> element(s) having their state attribute set to "terminated" (i.e. all public user identities are deregistered) and the Subscription-State header set to "terminated" or when all public user identities of the UE have been deregistered, the P-CSCF shall shorten the security associations towards the UE.

NOTE 1: The security association between the P-CSCF and the UEis shortened to a value that will allow the NOTIFY request containing the deregistration event to reach the UE.

NOTE 2: When the P-CSCF receives the NOTIFY request with Subscription-State header containing the value of "terminated", the P-CSCF considers the subscription to the reg event package terminated (i.e. as if the P-CSCF had sent a SUBSCRIBE request to the S-CSCF with an Expires header containing a value of zero).

## 5.2.6 General treatment for all dialogs and standalone transactions excluding the REGISTER method

### 5.2.6.1 Introduction

The procedures of subclause 5.2.6 and its subclauses are general to all requests and responses, except those for the REGISTER method.

### 5.2.6.2 Determination of mobile-originated or mobile-terminated case

Upon receipt of an initial request or a target refresh request or a stand-alone transaction, the P-CSCF shall:

- perform the procedures for the mobile-terminating case as described in subclause 5.2.6.4 if the request makes use of the information for mobile-terminating calls, which was added to the Path header entry of the P-CSCF during registration (see subclause 5.2.2), e.g. the message is received at a certain port or the topmost Route header contains a specific user part or parameter;

- perform the procedures for the mobile-originating case as described in subclause 5.2.6.3 if this information is not used by the request.

### 5.2.6.3 Requests initiated by the UE

When the P-CSCF receives an initial request for a dialog or a request for a standalone transaction, and the request contains a P-Preferred-Identity header that matches one of the registered public user identities, the P-CSCF shall identify the initiator of the request by that public user identity.

When the P-CSCF receives an initial request for a dialog or a request for a standalone transaction, and the request contains a P-Preferred-Identity header that does not match one of the registered public user identities, or does not contain a P-Preferred-Identity header, the P-CSCF shall identify the initiator of the request by a default public user identity. If there is more then one default public user identity available, the P-CSCF shall randomly select one of them.

NOTE 1: The contents of the From header do not form any part of this decision process.

When the P-CSCF receives from the UE an initial request for a dialog, and a Service-Route header list exists for the initiator of the request, the P-CSCF shall:

1) verify that the list of URIs received in the Service-Route header (during the last successful registration or re-registration) matches the preloaded Route headers in the received request. This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCFshall either:

   a) return a 400 (Bad Request) response; the P-CSCF shall not forward the request, and shall not continue with the execution of steps 2 onwards; or

   b) replace the preloaded Route header value in the request with the value of the Service-Route header received during the last 200 (OK) response for a registration or reregistration;

2) add its own address to the Via header. The P-CSCF Via header entry is built in a format that contains the port number of the P-CSCF in accordance with the procedures of RFC3261 [26], and either:

   a) the P-CSCF FQDN that resolves to the IP address, or

b) the P-CSCF IP address;

3) when adding its own SIP URI to the top of the Record-Route header, build the P-CSCF SIP URI in a format that contains the port number of the P-CSCF where it awaits subsequent requests from the called party, and either:

a) the P-CSCF FQDN that resolves to the IP address; or

b) the P-CSCF IP address;

4) remove the P-Preferred-Identity header, if present, and insert a P-Asserted-Identity header with a value representing the initiator of the request;

5) add a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.260 [17]; and

6) if the request is an INVITE request, save the Contact, CSeq and Record-Route header field values received in the request such that the P-CSCF is able to release the session if needed;

before forwarding the request, based on the topmost Route header, in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives a 1xx or 2xx response to the above request, the P-CSCF shall:

1) store the values received in the P-Charging-Function-Addresses header;

2) store the list of Record-Route headers from the received response;

3) store the dialog ID and associate it with the private user identity and public user identity involved in the session;

4) rewrite the port number of its own Record Route entry to its own protected server port number negotiated with the calling UE, and append the comp parameter in accordance with the procedures of RFC 3486 [55]; and

NOTE 2: The P-CSCF associates two ports, a protected client port and a protected server port, with each pair of security associations. For details on the selection of the protected port values see 3GPP TS 33.203 [19].

5) if the response corresponds to an INVITE request, save the Contact, From, To and Record-Route header field values received in the response such that the P-CSCF is able to release the session if needed;

before forwarding the response to the UE in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives from the UE a target refresh request for a dialog, the P-CSCF shall:

1) verify if the request relates to a dialog in which the originator of the request is involved:

a) if the request does not relates to an existing dialog in which the originator is involved, then the P-CSCF shall answer the request by sending a 403 (Forbidden) response back to the originator. The P-CSCF will not forward the request. No other actions are required; or

b) if the request relates to an existing dialog in which the originator is involved, then the P-CSCF shall continue with the following steps;

2) verify that the list of Route headers in the request matches the stored list of Record-Route headers for the same dialog. This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCF shall either:

a) return a 400 (Bad Request) response; the P-CSCF shall not forward the request, and shall not continue with the execution of steps 3 onwards; or

b) replace the Route header value in the request with the stored list of Record-Route headers for the same dialog;

3) add its own address to the Via header. The P-CSCF Via header entry is built in a format that contains the port number of the P-CSCF where it awaits the responses to come, and either:

a) the P-CSCF FQDN that resolves to the IP address, or

b) the P-CSCF IP address;

4) when adding its own SIP URI to the top of Record-Route header, build the P-CSCF SIP URI in a format that contains the port number of the P-CSCF where it awaits subsequent requests from the called party, and either:

   a) the P-CSCF FQDN that resolves to the IP address; or

   b) the P-CSCF IP address; and

5) for INVITE dialogs (i.e. dialogs initiated by an INVITE request), replace the saved Contact and Cseq header filed values received in the request such that the P-CSCF is able to release the session if needed;

NOTE 3: The replaced Contact header field value is valid only if a 1xx or 2xx response will be received for the request. In other cases the old value is still valid.

before forwarding the request, based on the topmost Route header, in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives a 1xx or 2xx response to the above request, the P-CSCF shall:

1) rewrite the port number of its own Record Route entry to the same value as for the response to the initial request for the dialog, and append the comp parameter in accordance with the procedures of RFC 3486 [55]; and

2) replace the saved Contact header value received in the response such that the P-CSCF is able to release the session if needed;

before forwarding the response to the UE in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives from the UE the request for a standalone transaction, and a Service-Route header list exists for the initiator of the request, the P-CSCF shall:

1) verify that the list of URIs received in the Service-Route header (during the last successful registration or re-registration) matches the preloaded Route headers in the received request. This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCF shall either:

   a) return a 400 (Bad Request) response; the P-CSCF shall not forward the request, and shall not continue with the execution of steps 3 onwards; or

   b) replace the preloaded Route header value in the request with the one received during the last registration in the Service-Route header of the 200 (OK) response;

2) remove the P-Preferred-Identity header, if present, and insert a P-Asserted-Identity header with a value representing the initiator of the request; and

3) add a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.260 [17];

before forwarding the request, based on the topmost Route header, in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives any response to the above request, the P-CSCF shall:

1) store the values received in the P-Charging-Function-Addresses header;

before forwarding the response to the UE in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives from the UE subsequent requests other than a target refresh request (including requests relating to an existing dialog where the method is unknown), the P-CSCF shall:

1) verify if the request relates to a dialog in which the originator of the request is involved:

   a) if the request does not relates to an existing dialog in which the originator is involved, then the P-CSCF shall answer the request by sending a 403 (Forbidden) response back to the originator. The P-CSCF will not forward the request. No other actions are required; or

   b) if the request relates to an existing dialog in which the originator is involved, then the P-CSCF shall continue with the following steps;

2) verify that the list of Route headers in the request matches the stored list of Record-Route headers for the same dialog. This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCF shall either:

a) return a 400 (Bad Request) response; the P-CSCF shall not forward the request, and shall not continue with the execution of steps 3 onwards; or

b) replace the Route header value in the request with the stored list of Record-Route headers for the same dialog;

3) for dialogs that are not INVITE dialogs, add a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.260 [17]; and

4) for INVITE dialogs, replace the saved Cseq header value received in the request such that the P-CSCF is able to release the session if needed;

before forwarding the request, (based on the topmost Route header,) in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives from the UE the request for an unknown method (that does not relate to an existing dialog), and a Service-Route header list exists for the initiator of the request, the P-CSCF shall:

1) verify that the list of URIs received in the Service-Route header (during the last successful registration or re-registration) is included, preserving the same order, as a subset of the preloaded Route headers in the received request. This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCF shall either:

a) return a 400 (Bad Request) response; the P-CSCF shall not forward the request, and shall not continue with the execution of steps 2 onwards; or

b) replace the Route header value in the request with the one received during the last registration in the Service-Route header of the 200 (OK) response; and

2) remove the P-Preferred-Identity header, if present, and insert a P-Asserted-Identity header with a value representing the initiator of the request;

before forwarding the request, based on the topmost Route header, in accordance with the procedures of RFC 3261 [26].

#### 5.2.6.4 Requests terminated by the UE

When the P-CSCF receives, destined for the UE, an initial request for a dialog, prior to forwarding the request, the P-CSCF shall:

1) convert the list of Record-Route header values into a list of Route header values and save this list of Route headers;

2) if the request is an INVITE request, save a copy of the Contact, CSeq and Record-Route header field values received in the request such that the P-CSCF is able to release the session if needed;

3) when adding its own SIP URI to the top of the list of Record-Route headers and save the list, build the P-CSCF SIP URI in a format that contains the comp parameter in accordance with the procedures of RFC 3486 [55], and the protected server port number of the security association established from the UE to the P-CSCF and either:

a) the P-CSCF FQDN that resolves to the IP address of the security association established from the UE to the P-CSCF; or

b) the P-CSCF IP address of the security association established from the UE to the P-CSCF;

4) when adding its own address to the top of the received list of Via header and save the list, build the P-CSCF Via header entry in a format that contains the comp parameter in accordance with the procedures of RFC 3486 [55], and the protected server port number of the security association established from the UE to the P-CSCF and either:

a) the P-CSCF FQDN that resolves to the IP address of the security association established from the UE to the P-CSCF; or

b) the P-CSCF IP address of the security association established from the UE to the P-CSCF;

NOTE 1: The P-CSCF associates two ports, a protected client port and a protected server port, with each pair of security associations. For details of the usage of the two ports see 3GPP TS 33.203 [19].

5) remove and store the values received in the P-Charging-Function-Addresses header;

6) remove and store the icid parameter received in the P-Charging-Vector header; and

7) save a copy of the P-Called-Party-ID header;

before forwarding the request to the UE in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives a 1xx or 2xx response to the above request, the P-CSCF shall:

1) remove the P-Preferred-Identity header, if present, and insert a P-Asserted-Identity header with the value saved from the P-Called-Party-ID header that was received in the request;

2) verify that the list of Via headers matches the saved list of Via headers received in the request corresponding to the same dialog, including the P-CSCF via header value. This verification is done on a per Via header value basis, not as a whole string. If the verification fails, then the P-CSCF shall either:

   a) discard the response; or

   b) replace the Via header values with those received in the request;

3) verify that the list of URIs received in the Record-Route header of the request corresponding to the same dialog is included, preserving the same order, as a subset of the Record-Route header list of this response. This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCF shall either:

   a) discard the response; or

   b) replace the Record-Route header values with those received in the request, rewrite the port number of its own Record-Route entry to the port number where it awaits subsequent requests from the calling party and remove the comp parameter.

      If the verification is successful, the P-CSCF shall rewrite the port number of its own Record-Route entry to the port number where it awaits subsequent requests from the calling party and remove the comp parameter;

4) store the dialog ID and associate it with the private user identity and public user identity involved in the session; and

5) if the response corresponds to an INVITE request, save the Contact, To, From and Record-Route header field value received in the response such that the P-CSCF is able to release the session if needed;

before forwarding the response in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives any other response to the above request, the P-CSCF shall:

1) verify that the list of Via headers matches the saved list of Via headers received in the request corresponding to the same dialog, including the P-CSCF via header value. This verification is done on a per Via header value basis, not as a whole string. If these lists do not match, then the P-CSCF shall either:

   a) discard the response; or

   b) replace the Via header values with those received in the request;

before forwarding the response in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives, destined for the UE, a target refresh request for a dialog, prior to forwarding the request, the P-CSCF shall:

1) add its own address to the top of the received list of Via header and save the list. The P-CSCF Via header entry is built in a format that contains the comp parameter in accordance with the procedures of RFC 3486 [55], and the protected server port number of the security association established from the UE to the P-CSCF and either:

   a) the P-CSCF FQDN that resolves to the IP address of the security association established from the UE to the P-CSCF; or

b) the P-CSCF IP address of the security association established from the UE to the P-CSCF;

NOTE 2: The P-CSCF associates two ports, a protected client port and a protected server port, with each pair of security associations. For details of the usage of the two ports see 3GPP TS 33.203 [19].

2) when adding its own SIP URI to the top of the list of Record-Route headers and save the list, build the P-CSCF SIP URI in a format that contains the comp parameter in accordance with the procedures of RFC 3486 [55], and the protected server port number of the security association established from the UE to the P-CSCF and either:

   a) the P-CSCF FQDN that resolves to the IP address of the security association established from the UE to the P-CSCF; or

   b) the P-CSCF IP address of the security association established from the UE to the P-CSCF; and

3) for INVITE dialogs, replace the saved Contact and Cseq header field values received in the request such that the P-CSCF is able to release the session if needed;

NOTE 3: The replaced Contact header field value is valid only if a 1xx or 2xx response will be received for the request. In other cases the old value is still valid.

before forwarding the request to the UE in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives a 1xx or 2xx response to the above request, the P-CSCF shall:

1) verify that the list of Via headers matches the saved list of Via headers received in the request corresponding to the same dialog, including the P-CSCF via header value. This verification is done on a per Via header value basis, not as a whole string. If the verification fails, then the P-CSCF shall either:

   a) discard the response; or

   b) replace the Via header values with those received in the request;

2) rewrite the port number of its own Record-Route entry to the same value as for the response to the initial request for the dialog and remove the comp parameter; and

3) replace the saved Contact header field value received in the response such that the P-CSCF is able to release the session if needed;

before forwarding the response in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives any other response to the above request, the P-CSCF shall:

1) verify that the list of Via headers matches the saved list of Via headers received in the request corresponding to the same dialog, including the P-CSCF via header value. This verification is done on a per Via header value basis, not as a whole string. If the verification fails, then the P-CSCF shall either:

   a) discard the response; or

   b) replace the Via header values with those received in the request; and

2) rewrite the port number of its own Record-Route entry to the port number where it awaits subsequent requests from the calling party and remove the comp parameter;

before forwarding the response in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives, destined for the UE, a request for a standalone transaction, or a request for an unknown method (that does not relate to an existing dialog), prior to forwarding the request, the P-CSCF shall:

1) add its own address to the top of the received list of Via header and save the list. The P-CSCF Via header entry is built in a format that contains the comp parameter in accordance with the procedures of RFC 3486 [55], and the protected server port number of the security association established from the UE to the P-CSCF and either:

   a) the P-CSCF FQDN that resolves to the IP address of the security association established from the UE to the P-CSCF; or

   b) the P-CSCF IP address of the security association established from the UE to the P-CSCF;

NOTE 4: The P-CSCF associates two ports, a protected client port and a protected server port, with each pair of security associations. For details of the usage of the two ports see 3GPP TS 33.203 [19].

2) store the values received in the P-Charging-Function-Addresses header;

3) remove and store the icid parameter received in the P-Charging-Vector header; and

4) save a copy of the P-Called-Party-ID header;

before forwarding the request to the UE in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives any response to the above request, the P-CSCF shall:

1) verify that the list of Via headers matches the saved list of Via headers received in the request corresponding to the same dialog, including the P-CSCF via header value. This verification is done on a per Via header value basis, not as a whole string. If these lists do not match, then the P-CSCF shall either:

   a) discard the response; or

   b) replace the Via header values with those received in the request; and

2) remove the P-Preferred-Identity header, if present, and insert an P-Asserted-Identity header with the value saved from the P-Called-Party-ID header of the request;

before forwarding the response in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives, destined for the UE, a subsequent request for a dialog that is not a target refresh request (including requests relating to an existing dialog where the method is unknown), prior to forwarding the request, the P-CSCF shall:

1) add its own address to the top of the received list of Via header and save the list The P-CSCF Via header entry is built in a format that contains the comp parameter in accordance with the procedures of RFC 3486 [55], and the protected server port number of the security association established from the UE to the P-CSCF and either:

   a) the P-CSCF FQDN that resolves to the IP address of the security association established from the UE to the P-CSCF; or

   b) the P-CSCF IP address of the security association established from the UE to the P-CSCF;

NOTE 5: The P-CSCF associates two ports, a protected client port and a protected server port, with each pair of security associations. For details of the usage of the two ports see 3GPP TS 33.203 [19].

2) remove and store the icid parameter from P-Charging-Vector header; and

3) for INVITE dialogs, replace the saved Cseq header value received in the request such that the P-CSCF is able to release the session if needed;

before forwarding the request to the UE in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives any response to the above request, the P-CSCF shall:

1) verify that the list of Via headers matches the saved list of Via headers received in the request corresponding to the same dialog, including the P-CSCF via header value. This verification is done on a per Via header value basis, not as a whole string. If these lists do not match, then the P-CSCF shall either:

   a) discard the response; or

   b) replace the Via header values with those received in the request;

before forwarding the response in accordance with the procedures of RFC 3261 [26].

## 5.2.7 Initial INVITE

### 5.2.7.1 Introduction

In addition to following the procedures for initial requests defined in subclause 5.2.6, initial INVITE requests also follow the procedures of this subclause.

### 5.2.7.2 Mobile-originating case

When the P-CSCF receives from the UE an INVITE request, the P-CSCF may require the periodic refreshment of the session to avoid hung states in the P-CSCF. If the P-CSCF requires the session to be refreshed, it shall apply the procedures described in RFC 4028 [58] clause 8.

NOTE 1: Requesting the session to be refreshed requires support by at least one of the UEs. This functionality cannot automatically be granted, i.e. at least one of the involved UEs needs to support it.

The P-CSCF shall respond to all INVITE requests with a 100 (Trying) provisional response.

Upon receiving a response as specified in RFC 3313 [31] to the initial INVITE request, the P-CSCF shall:

- if a media authorization token is generated by the PDF (i.e. when service-based local policy control is applied), insert the P-Media-Authorization header containing that media authorization token.

NOTE 2: Typically, the first 183 (Session Progress) response contains an SDP answer including one or more "m=" media descriptions, but it is also possible that the response does not contain an SDP answer or the SDP does not include at least an "m=" media description. However, the media authorization token is generated independently of the presence or absence of "m=" media descriptions and sent to the UE in the P-Media-Authorization header value. The same media authorization token is used until the session is terminated. For further details see 3GPP TS 29.207 [12].

The P-CSCF shall also include the access-network-charging-info parameter (if received via the PDF, over the Go and Gq interfaces) in the P-Charging-Vector header in the first request originated by the UE that traverses the P-CSCF, as soon as the charging information is available in the P-CSCF, e.g., after the local resource reservation is complete. Typically, this first request is an UPDATE request if the remote UA supports the "integration of resource management in SIP" extension or a re-INVITE request if the remote UA does not support the "integration of resource management in SIP" extension. See subclause 5.2.7.4 for further information on the access network charging information.

### 5.2.7.3 Mobile-terminating case

When the P-CSCF receives an INVITE request destined for the UE the P-CSCF may require the periodic refreshment of the session to avoid hung states in the P-CSCF. If the P-CSCF requires the session to be refreshed, it shall apply the procedures described in draft-ietf-sip-session-timer [58] clause 8.

NOTE 1: Requesting the session to be refreshed requires support by at least one of the UEs. This functionality cannot automatically be granted, i.e. at least one of the involved UEs needs to support it in order to make it work.

When the P-CSCF receives an initial INVITE request destined for the UE, it will contain the URI of the UE in the Request-URI, and a single preloaded Route header. The received initial INVITE request will also have a list of Record-Route headers. Prior to forwarding the initial INVITE to the URI found in the Request-URI, the P-CSCF shall:

- if a media authorization token is generated by the PDF as specified in RFC 3313 [31] (i.e. when service-based local policy control is applied), insert the P-Media-Authorization header containing that media authorization token.

NOTE 2: Typically, the initial INVITE request contains an SDP offer including one or more "m=" media descriptions, but it is also possible that the INVITE request does not contain an SDP offer or the SDP does not include at least an "m= media description. However, the media authorization token is generated independently of the presence or absence of "m=" media descriptions and sent to the UE in the P-Media-Authorization header value. The same media authorization token is used until the session is terminated. For further details see 3GPP TS 29.207 [12].

In addition, the P-CSCF shall respond to all INVITE requests with a 100 (Trying) provisional response.

The P-CSCF shall also include the access-network-charging-info parameter (if received via the PDF, over the Go and Gq interfaces) in the P-Charging-Vector header in the first request or response originated by the UE that traverses the P-CSCF, as soon as the charging information is available in the P-CSCF e.g., after the local resource reservation is complete. Typically, this first response is a 180 (Ringing) or 200 (OK) response if the remote UA supports the "integration of resource management in SIP" extension, or a re-INVITE request if the remote UA does not support the "integration of resource management in SIP" extension. See subclause 5.2.7.4 for further information on the access network charging information.

#### 5.2.7.4 Access network charging information

The P-CSCF shall include the access-network-charging-info parameter within the P-Charging-Vector header as described in subclause 7.2A.5.

## 5.2.8 Call release

### 5.2.8.1 P-CSCF-initiated call release

#### 5.2.8.1.1 Cancellation of a session currently being established

Upon receipt of an indication that radio coverage is no longer available for a multimedia session currently being established (e.g. abort session request from PDF), the P-CSCF shall cancel that dialog by sending out a CANCEL request according to the procedures described in RFC 3261 [26].

#### 5.2.8.1.2 Release of an existing session

Upon receipt of an indication that the radio interface resources are no longer available for a session (e.g. abort session request from PDF), the P-CSCF shall release that dialog by applying the following steps:

1) if the P-CSCF serves the calling user of the session it shall generate a BYE request based on the information saved for the related dialog, including:

   - a Request-URI, set to the stored Contact header provided by the called user;
   - a To header, set to the To header value as received in the 200 (OK) response for the initial INVITE request;
   - a From header, set to the From header value as received in the initial INVITE request;
   - a Call-ID header, set to the Call-Id header value as received in the initial INVITE request;
   - a CSeq header, set to the current CSeq value stored for the direction from the calling to the called user, incremented by one;
   - a Route header, set to the routeing information towards the called user as stored for the dialog;
   - further headers, based on local policy or the requested session release reason.

2) If the P-CSCF serves the called user of the session it shall generate a BYE request based on the information saved for the related dialog, including:

   - a Request-URI, set to the stored Contact header provided by the calling user;
   - a To header, set to the From header value as received in the initial INVITE request;
   - a From header, set to the To header value as received in the 200 (OK) response for the initial INVITE request;
   - a Call-ID header, set to the Call-Id header value as received in the initial INVITE request;
   - a CSeq header, set to the current CSeq value stored for the direction from the called to the calling user, incremented by one;
   - a Route header, set to the routeing information towards the calling user as stored for the dialog;

- further headers, based on local policy or the requested session release reason.

3) send the so generated BYE request towards the indicated user.

4) upon receipt of the 2xx responses for the BYE request, shall delete all information related to the dialog and the related multimedia session.

#### 5.2.8.1.3 Abnormal cases

Upon receipt of a request on a dialog for which the P-CSCF initiated session release, the P-CSCF shall terminate this received request and answer it with a 481 (Call/Transaction Does Not Exist) response.

#### 5.2.8.1.4 Release of the existing dialogs due to registration expiration and deletion of the security association

If there are still active dialogs associated with the user after the security associations were deleted, the P-CSCF shall discard all information pertaining to these dialogs without performing any further SIP transactions with the peer entities of the P-CSCF.

NOTE: At the same time, the P-CSCF will also indicate via the Gq interface that the session has been terminated.

### 5.2.8.2 Call release initiated by any other entity

When the P-CSCF receives a 2xx response for a BYE request matching an existing dialog, it shall delete all the stored information related to the dialog.

### 5.2.8.3 Session expiration

If the P-CSCF requested the session to be refreshed periodically, and the P-CSCF got the indication that the session will be refreshed, when the session timer expires, the P-CSCF shall delete all the stored information related to the dialog.

NOTE: The P-CSCF will also indicate to the IP-CAN, via the Gq interface, that the session has terminated.

## 5.2.9 Subsequent requests

### 5.2.9.1 Mobile-originating case

The P-CSCF shall respond to all reINVITE requests with a 100 (Trying) provisional response.

For a reINVITE request or UPDATE request from the UE within the same dialog, the P-CSCF shall include the updated access-network-charging-info parameter from P-Charging-Vector header when sending the SIP request to the S-CSCF. See subclause 5.2.7.4 for further information on the access network charging information.

### 5.2.9.2 Mobile-terminating case

The P-CSCF shall respond to all reINVITE requests with a 100 (Trying) provisional response.

For a reINVITE request or UPDATE request destined towards the UE within the same dialog, when the P-CSCF sends 200 (OK) response (to the INVITE request or UPDATE request) towards the S-CSCF, the P-CSCF shall include the updated access-network-charging-info parameter in the P-Charging-Vector header. See subclause 5.2.7.4 for further information on the access network charging information.

## 5.2.10 Emergency service

The P-CSCF shall store a configurable list of local emergency numbers and emergency URIs, i.e. those used for emergency services by the operator to which the P-CSCF belongs to. In addition to that, the P-CSCF shall store a configurable list of roaming partners' emergency numbers and emergency URIs associated with MCC and MNC codes.

NOTE: Certain SIP URIs may be classified as emergency URIs in all networks.

The P-CSCF shall inspect the Request URI of all INVITE requests from the UE for known emergency numbers and emergency URIs from these configurable lists. If the P-CSCF detects that the Request-URI of the INVITE request matches one of the numbers in any of these lists, the P-CSCF shall not forward the INVITE request. The P-CSCF shall respond the INVITE request with a 380 (Alternative Service) response.

In order to determine whether the INVITE request is destined for an emergency centre in the roaming country (i.e. the list of roaming partners' are inspected), the P-CSCF shall compare the MCC and the MNC fields in the received in the P-Access-Network-Info header of the INVITE request against its own MCC and MNC codes.

The P-CSCF shall include in the 380 (Alternative Service) response a Content-Type header field with the value set to associated MIME type of the 3GPP IMS XML body as described in subclause 7.6.1.

The P-CSCF shall include in the 3GPP IMS XML body:

a) an <alternative-service> element, set to the parameters of the alternative service:

b) a <type> child element, set to "emergency" to indicate that it was an emergency call; and

c) a <reason> child element, set to an operator configurable reason.

### 5.2.11 Void

## 5.3 Procedures at the I-CSCF

### 5.3.1 Registration procedure

#### 5.3.1.1 General

During the registration procedure the I-CSCF shall behave as a stateful proxy.

#### 5.3.1.2 Normal procedures

When I-CSCF receives a REGISTER request, the I-CSCF starts the user registration status query procedure to the HSS as specified in 3GPP TS 29.228 [14].

NOTE: Different UEs, each with its own private user identity, may register the same shared public user identity. Registrations of all public user identities belonging to these UEs are directed to the same S-CSCF as described in 3GPP TS 29.228 [14].

Prior to performing the user registration query procedure to the HSS, the I-CSCF decides which HSS to query, possibly as a result of a query to the Subscription Locator Functional (SLF) entity as specified in 3GPP TS 29.228 [14].

If the user registration status query response from the HSS includes a valid SIP URI, the I-CSCF shall:

1) replace the Request-URI of the received REGISTER request with the SIP URI received from the HSS in the Server-Name AVP;

2) apply the procedures as described in subclause 5.3.3 if topology hiding is required; and

3) forward the REGISTER request to the indicated S-CSCF.

If the user registration status query response from the HSS includes a list of capabilities, the I-CSCF shall:

1) select a S-CSCF that fulfils the indicated mandatory capabilities – if more then one S-CSCFs fulfils the indicated mandatory capabilities the S-CSCF which fulfils most of the possibly additionally indicated optional capabilities;

2) replace the Request-URI of the received REGISTER request with the URI of the S-CSCF;

3) apply the procedures as described in subclause 5.3.3 if topology hiding is required; and

4) forward the REGISTER request to the selected S-CSCF.

If the user registration status query response from the HSS includes both a list of capabilities and a valid SIP URI, the I-CSCF shall first use the SIP URI to select the S-CSCF, and then if the S-CSCF is not reachable, the I-CSCF shall select a new S-CSCF as indicated in the abnormal cases of subclause 5.3.1.3.

When the I-CSCF receives a 2xx response to a REGISTER request, the I-CSCF shall proxy the 2xx response to the P-CSCF.

### 5.3.1.3 Abnormal cases

In the case of SLF query, if the SLF does not send HSS address to the I-CSCF, the I-CSCF shall send back a 403 (Forbidden) response to the UE.

If the HSS sends a negative response to the user registration status query request, the I-CSCF shall send back a 403 (Forbidden) response.

If the the user registration status query procedure cannot be completed, e.g. due to time-out or incorrect information from the HSS, the I-CSCF shall send back a 480 (Temporarily Unavailable) response to the UE.

If a selected S-CSCF:

- does not respond to the REGISTER request and its retransmissions by the I-CSCF; or
- sends back a 3xx response or 480 (Temporarily Unavailable) response to a REGISTER request;

and:

- the REGISTER request did not include an "integrity-protected" parameter in the Authorization header; or
- did include an "integrity-protected" parameter with a value different from "yes" in the Authorization header;

then:

- if the I-CSCF has received the list of capabilities from the HSS, the I-CSCF shall select a new S-CSCF as described in subclause 5.3.1.2, based on the capabilities indicated from the HSS. The newly selected S-CSCF shall not be one of any S-CSCFs selected previously during this same registration procedure; or
- if the I-CSCF has received a valid SIP URI from the HSS because the S-CSCF is already assigned to other UEs sharing the same public user identity, it will request the list of capabilities from the HSS and, on receiving these capabilities, the I-CSCF shall select a new S-CSCF as described in subclause 5.3.1.2, based on the capabilities indicated from the HSS. The newly selected S-CSCF shall not be one of any S-CSCFs selected previously during this same registration procedure.

If a selected S-CSCF does not respond to a REGISTER request and its retransmissions by the I-CSCF and the REGISTER request did include an Authorization header with the "integrity-protected" parameter set to "yes", the I-CSCF shall send back a 408 (Request Timeout) response or 504 (Server Time-Out) response to the user, in accordance with the procedures in RFC 3261 [26].

If the I-CSCF cannot select a S-CSCF which fulfils the mandatory capabilities indicated by the HSS, the I-CSCF shall send back a 600 (Busy Everywhere) response to the user.

## 5.3.2 Initial requests

### 5.3.2.1 Normal procedures

The I-CSCF may behave as a stateful proxy for initial requests.

The I-CSCF shall verify for all requests whether they arrived from a trusted domain or not. If the request arrived from a non trusted domain, then the I-CSCF shall:

1) respond with 403 (Forbidden) response if the request is a REGISTER request;
2) remove all P-Asserted-Identity headers, all P-Access-Network-Info headers, all P-Charging-Vector headers and all P-Charging-Function-Addresses headers the request may contain, if the request is other than REGISTER request; and

3) continue with the procedures below.

If the request arrived from a trusted domain, the I-CSCF shall perform the procedures below.

NOTE 1: The I-CSCF may find out whether the request arrived from a trusted domain or not, from the procedures described in 3GPP TS 33.210 [19A].

When the I-CSCF receives an initial request for a dialog or standalone transaction the I-CSCF shall:

1) if the Request-URI includes a pres: or an im: URI, then translate the pres: or im: URI to a public user identity and replace the Request-URI of the incoming request with that public user identity; and

NOTE 2: SRV records have to be advertised in DNS pointing to the I-CSCF for pres: and im: queries.

2) if the request does not contain a Route header, then check if the domain name of the Request-URI matches with one of the PSI subdomains configured in the I-CSCF. If the match is successful, the I-CSCF resolves the Request-URI by an internal DNS mechanism into the IP address of the AS hosting the PSI and does not start the user location query procedure. Otherwise, the I-CSCF shall start the user location query procedure to the HSS as specified in 3GPP TS 29.228 [14] for the called user, indicated in the Request-URI. Prior to performing the user location query procedure to the HSS, the I-CSCF decides which HSS to query, possibly as a result of a query to the Subscription Locator Functional (SLF) entity as specified in 3GPP TS 29.228 [14].

When the S-CSCF receives any response to such a request request, the S-CSCF shall store the value of the term-ioi parameter received in the P-Charging-Vector header, if present.

NOTE 3: Any received term-ioi parameter will be a type 3 term-ioi. The type 3 term-ioi identifies the service provider from which the response was sent.

When the I-CSCF receives an INVITE request, the I-CSCF may require the periodic refreshment of the session to avoid hung states in the I-CSCF. If the I-CSCF requires the session to be refreshed, it shall apply the procedures described in RFC 4028 [58] clause 8.

NOTE 4: Requesting the session to be refreshed requires support by at least one of the UEs. This functionality cannot automatically be granted, i.e. at least one of the involved UEs needs to support it.

In case the I-CSCF is able to resolve the Request-URI into the IP address of the AS hosting the PSI, then it shall:

1) store the value of the icid parameter received in the P-Charging-Vector header and retain the icid parameter in the P-Charging-Vector header. If no icid parameter was found, then create a new, globally unique value for the icid parameter and insert it into the P-Charging-Vector header;

2) apply the procedures as described in subclause 5.3.3 if topology hiding is required; and

3) forward the request directly to the AS hosting the PSI.

Upon successful user location query, when the response contains the URI of the assigned S-CSCF, the I-CSCF shall:

1) insert the URI received from the HSS as the topmost Route header;

2) store the value of the icid parameter received in the P-Charging-Vector header and retain the icid parameter in the P-Charging-Vector header. If no icid parameter was found, then create a new, globally unique value for the icid parameter and insert it into the P-Charging-Vector header;

3) apply the procedures as described in subclause 5.3.3 if topology hiding is required; and

4) forward the request based on the topmost Route header.

Upon successful user location query, when the response contains information about the required S-CSCF capabilities, the I-CSCF shall:

1) select a S-CSCF according to the method described in 3GPP TS 29.228 [14];

2) insert the URI of the selected S-CSCF as the topmost Route header field value;

3) execute the procedure described in step 2 and 3 in the above paragraph (upon successful user location query, when the response contains the URI of the assigned S-CSCF); and

4) forward the request to the selected S-CSCF.

Upon an unsuccessful user location query when the response from the HSS indicates that the user does not exist, the I-CSCF shall return an appropriate unsuccessful SIP response. This response may be a 404 (Not found) or 604 (Does not exist anywhere) in the case the user is not a user of the home network.

Upon an unsuccessful user location query when the response from the HSS indicates that the user is not registered and no services are provided for such a user, the I-CSCF shall return an appropriate unsuccessful SIP response. This response may be a 480 (Temporarily unavailable) if the user is recognized as a valid user, but is not registered at the moment and it does not have services for unregistered users.

When the I-CSCF receives an initial request for a dialog or standalone transaction, that contains a single Route header pointing to itself, the I-CSCF shall determine from the entry in the Route header whether it needs to do HSS query or hiding. In case HSS query is needed, then the I-CSCF shall perform the procedures described for the case when there is no Route header present. If the I-CSCF determines that hiding must be performed for an outgoing request, and the I-CSCF shall:

1) remove its own SIP URI from the topmost Route header;

2) perform the procedures described in subclause 5.3.3; and

3) route the request based on the Request-URI header field.

When the I-CSCF receives an initial request for a dialog or standalone transaction containing more than one Route header, the I-CSCF shall:

1) remove its own SIP URI from the topmost Route header;

2) apply the procedures as described in subclause 5.3.3; and

3) forward the request based on the topmost Route header.

NOTE 5: In accordance with SIP the I-CSCF can add its own routeable SIP URI to the top of the Record-Route header to any request, independently of whether it is an initial request, or whether topology hiding is performed. The P-CSCF will ignore any Record-Route header that is not in the initial request of a dialog.

When the I-CSCF receives a response to an initial request (e.g. 183 or 2xx), the I-CSCF shall store the values from the P-Charging-Function-Addresses header, if present. If the next hop is outside of the current network, then the I-CSCF shall remove the P-Charging-Function-Addresses header prior to forwarding the message.

When the I-CSCF, upon sending an initial INVITE request to the S-CSCF, receives a 305 (Use Proxy) response from the S-CSCF, it shall forward the initial INVITE request to the SIP URI indicated in the Contact field of the 305 (Use Proxy) response, as specified in RFC 3261 [26].

#### 5.3.2.2 Abnormal cases

In the case of SLF query, if the SLF does not send HSS address to the I-CSCF, the I-CSCF shall send back a 404 (Not Found) response to the UE.

If the I-CSCF receives a negative response to the user location query, the I-CSCF shall send back a 404 (Not Found) response.

If the I-CSCF receives a CANCEL request and if the I-CSCF finds an internal state indicating a pending Cx transaction with the HSS, the I-CSCF:

- shall answer the CANCEL with a 200 OK; and

- shall answer the original request with a 487 Request Terminated.

NOTE: The I-CSCF will discard any later arriving (pending) Cx answer message from the HSS.

## 5.3.3 THIG functionality in the I-CSCF(THIG)

### 5.3.3.1 General

The following procedures shall only be applied if topology hiding is required by the network. The network requiring topology hiding is called the hiding network.

NOTE 1: Requests and responses are handled independently therefore no state information is needed for that purpose within an I-CSCF(THIG).

The I-CSCF(THIG) shall apply topology hiding to all headers which reveal topology information, such as Via, Route, Record-Route, Service-Route.

Upon receiving an incoming REGISTER request for which topology hiding has to be applied and which includes a Path header, the I-CSCF(THIG) shall add the routeable SIP URI of an I-CSCF(THIG) to the top of the Path header. The I-CSCF(THIG) may include in the inserted SIP URI an indicator that identifies the direction of subsequent requests received by the I-CSCF i.e., from the S-CSCF towards the P-CSCF, to identify the mobile-terminating case. The I-CSCF(THIG) may encode this indicator in different ways, such as, e.g., a unique parameter in the URI, a character string in the username part of the URI, or a dedicated port number in the URI.

NOTE 2: Any subsequent request that includes the direction indicator (in the Route header) or arrives at the dedicated port number, indicates that the request was sent by the S-CSCF towards the P-CSCF.

Upon receiving an incoming initial request for which topology hiding has to be applied and which includes a Record-Route header, the I-CSCF(THIG) shall add its own routeable SIP URI to the top of the Record-Route header.

Upon receiving an outgoing initial request for which topology hiding has to be applied and which includes P-Charging-Function-Addresses header, the I-CSCF(THIG) shall remove the P-Charging-Function-Addresses header prior to forwarding the message.

### 5.3.3.2 Encryption for topology hiding

Upon receiving an outgoing request/response from the hiding network the I-CSCF(THIG) shall perform the encryption for topology hiding purposes, i.e. the I-CSCF(THIG) shall:

1) use the whole header values which were added by one or more specific entity of the hiding network as input to encryption, besides the UE entry;

2) not change the order of the headers subject to encryption when performing encryption;

3) use for one encrypted string all received consecutive header entries subject to encryption, regardless if they appear in separate consecutive headers or if they are consecutive entries in a comma separated list in one header;

4) construct an NAI in the form of 'username@realm',where the username part is the encrypted string, and the realm is the name of the encrypting network.

5) append a "tokenized-by=" tag and set it to the value of the encrypting network's name, after the constructed NAI;

6) form one valid entry for the specific header out of the resulting NAI, e.g. prepend "SIP/2.0/UDP" for Via headers or "sip:" for Route and Record-Route headers.

NOTE 1: Even if consecutive entries of the same network in a specific header are encrypted, they will result in only one encrypted header entry. For example:

```
Via: SIP/2.0/UDP icscf1_s.home1.net;lr,
     SIP/2.0/UDP Token( SIP/2.0/UDP scscf1.home1.net;lr,
                        SIP/2.0/UDP pcscf1.home1.net;lr)@home1.net;
                                    tokenized-by=home1.net,
     SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
```

NOTE 2: If multiple entries of the same network are within the same type of headers, but they are not consecutive, then these entries will be tokenized to different strings. For example:

```
Route:  sip:icscf1_s.home1.net;lr,
        sip:Token(sip:scscf1.home1.net;lr)@home1.net;tokenized-by=home1.net,
        sip:as1.foreign.net;lr,
        sip:Token(sip:scscf1.home1.net;lr,
                  sip:pcscf1.home1.net;lr)@home1.net;tokenized-by=home1.net,
        sip:[5555::aaa:bbb:ccc:ddd]
```

#### 5.3.3.3 Decryption for Topology Hiding

Upon receiving and incoming requests/response to the hiding network the I-CSCF(THIG) shall perform the decryption for topology hiding purposes, i.e. the I-CSCF shall:

1) identify NAIs encrypted by the network this I-CSCF belongs to within all headers of the incoming message;

2) use the user part of those NAIs that carry the identification of the hiding network within the value of the tokenized-by tag as input to decryption;

3) use as encrypted string the user part of the NAI which follows the sent-protocol (for Via Headers, e.g. "SIP/2.0/UDP") or the URI scheme (for Route and Record-Route Headers, e.g. "sip:");

4) replace all content of the received header which carries encrypted information with the entries resulting from decryption.

EXAMPLE: An encrypted entry to a Via header that looks like:

```
Via:    SIP/2.0/UDP Token(SIP/2.0/UDP scscf1.home1.net;lr,
        SIP/2.0/UDP pcscf1.home1.net;lr)@home1.net;tokenized-by=home1.net
```

will be replaced with the following entries:

```
Via: SIP/2.0/UDP scscf1.home1.net;lr, SIP/2.0/UDP pcscf1.home1.net;lr
```

NOTE: Motivations for these decryption procedures are e.g. to allow the correct routeing of a response through the hiding network, to enable loop avoidance within the hiding network, or to allow the entities of the hiding network to change their entries within e.g. the Record-Route header.

### 5.3.4 Void

## 5.4 Procedures at the S-CSCF

### 5.4.1 Registration and authentication

#### 5.4.1.1 Introduction

The S-CSCF shall act as the SIP registrar for all UAs belonging to the IM CN subsystem and with public user identities.

The S-CSCF shall support the use of the Path and Service-Route header. The S-CSCF shall also support the Require and Supported headers. The Path header is only applicable to the REGISTER request and its 200 (OK) response. The Service-Route header is only applicable to the 200 (OK) response of REGISTER.

The network operator defines minimum and maximum times for each registration. These values are provided within the S-CSCF.

The procedures for notification concerning automatically registered public user identities of a user are described in subclause 5.4.2.1.2.

### 5.4.1.2 Initial registration and user-initiated reregistration

#### 5.4.1.2.1 Unprotected REGISTER

NOTE 1: Any REGISTER request sent unprotected by the UE is considered to be an initial registration. A 200 (OK) final response to such a request will only be sent back after the S-CSCF receives a correct authentication challenge response in a REGISTER request that is sent integrity protected.

NOTE 2: A REGISTER with Expires header value equal to zero should always be received protected. However, it is possible that in error conditions a REGISTER with Expires header value equal to zero may be received unprotected. In that instance the procedures below will be applied.

Upon receipt of a REGISTER request without an "integrity-protected" parameter, or with the "integrity-protected" parameter in the Authorization header set to "no", for an already registered public user identity linked to the same private user identity but with a new contact information (e.g. a user roams to a different network without de-registering the previous one), the S-CSCF shall:

1) perform the procedure for receipt of a REGISTER request without an "integrity-protected" parameter, or with the "integrity-protected" parameter in the Authorization header set to "no"', for the received public user identity; and

2) if the authentication has been successful and if the previous registration has not expired, the S-CSCF shall perform the network initiated deregistration procedure only for the previous contact information as described in subclause 5.4.1.5.

Upon receipt of a REGISTER request without an "integrity-protected" parameter, or with the "integrity-protected" parameter in the Authorization header set to "no", which is not for an already registered public user identity linked to the same private user identity, the S-CSCF shall:

1) identify the user by the public user identity as received in the To header and the private user identity as received in the username field in the Authorization header of the REGISTER request;

2) check if the P-Visited-Network header is included in the REGISTER request, and if it is included identify the visited network by the value of this header;

3) select an authentication vector for the user. If no authentication vector for this user is available, after the S-CSCF has performed the Cx Multimedia Authentication procedure with the HSS, as described in 3GPP TS 29.228 [14], the S-CSCF shall select an authentication vector as described in 3GPP TS 33.203 [19].

   Prior to performing Cx Multimedia Authentication procedure with the HSS, the S-CSCF decides which HSS to query, possibly as a result of a query to the Subscription Locator Functional (SLF) entity as specified in 3GPP TS 29.228 [14];

NOTE 3: At this point the S-CSCF informs the HSS, that the user currently registering will be served by the S-CSCF by passing its SIP URI to the HSS. This will be used by the HSS to direct all subsequent incoming initial requests for a dialog or standalone transactions destined for this user to this S-CSCF.

NOTE 4: When passing its SIP URI to the HSS, the S-CSCF may include in its SIP URI the transport protocol and the port number where it wants to be contacted.

4) store the icid parameter received in the P-Charging-Vector header;

5) challenge the user by generating a 401 (Unauthorized) response for the received REGISTER request, including a WWW-Authenticate header which transports:

   - the home network identification in the realm field;

   - the RAND and AUTN parameters and optional server specific data for the UE in the nonce field;

   - the security mechanism, which is AKAv1-MD5, in the algorithm field;

   - the IK (Integrity Key) parameter for the P-CSCF in the ik field (see subclause 7.2A.1); and

   - the CK (Cipher Key) parameter for the P-CSCF in the ck field (see subclause 7.2A.1);

6) store the RAND parameter used in the 401 (Unathorized) response for future use in case of a resynchronisation. If a stored RAND already exists in the S-CSCF, the S-CSCF shall overwrite the stored RAND with the RAND used in the most recent 401 (Unauthorized) response;

7) send the so generated 401 (Unauthorized) response towards the UE; and,

8) start timer reg-await-auth which guards the receipt of the next REGISTER request.

If the received REGISTER request indicates that the challenge sent previously by the S-CSCF to the UE was deemed to be invalid by the UE, the S-CSCF shall stop the timer reg-await-auth and proceed as described in the subclause 5.4.1.2.3.

#### 5.4.1.2.2 Protected REGISTER

Upon receipt of a REGISTER request with the "integrity-protected" parameter in the Authorization header set to "yes", the S-CSCF shall identify the user by the public user identity as received in the To header and the private user identity as received in the Authorization header of the REGISTER request, and:

In the case that there is no authentication currently ongoing for this user (i.e. no timer reg-await-auth is running):

1) check if the user needs to be reauthenticated.

   The S-CSCF may require authentication of the user for any REGISTER request, and shall always require authentication for REGISTER requests received without the "integrity-protected" parameter in the Authorization header set to "yes".

   If the user needs to be reauthenticated, the S-CSCF shall proceed with the procedures as described for the initial REGISTER in subclause 5.4.1.2.1, beginning with step 4). If the user does not need to be reauthenticated, the S-CSCF shall proceed with the following steps in this paragraph; and

2) check whether an Expires timer is included in the REGISTER request and its value. If the Expires header indicates a zero value, the S-CSCF shall perform the deregistration procedures as described in subclause 5.4.1.4. If the Expires header does not indicate zero, the S-CSCF shall check whether the public user identity received in the To header is already registered. If it is not registered, the S-CSCF shall proceed beginning with step 5 below. Otherwise, the S-CSCF shall proceed beginning with step 6 below.

In the case that a timer reg-await-auth is running for this user the S-CSCF shall:

1) check if the Call-ID of the request matches with the Call-ID of the 401 (Unauthorized) response which carried the last challenge. The S-CSCF shall only proceed further if the Call-IDs match.

2) stop timer reg-await-auth;

3) check whether an Authorization header is included, containing:

   a) the private user identity of the user in the username field;

   b) the algorithm which is AKAv1-MD5 in the algorithm field; and

   c) the authentication challenge response needed for the authentication procedure in the response field.

   The S-CSCF shall only proceed with the following steps in this paragraph if the authentication challenge response was included;

4) check whether the received authentication challenge response and the expected authentication challenge response (calculated by the S-CSCF using XRES and other parameters as described in RFC 3310 [49]) match. The XRES parameter was received from the HSS as part of the Authentication Vector. The S-CSCF shall only proceed with the following steps if the challenge response received from the UE and the expected response calculated by the S-CSCF match;

5) after performing the Cx Server Assignment procedure with the HSS, as described in 3GPP TS 29.228 [14], store the following information in the local data:

   a) the list of public user identities associated to the the public user identity under registration, including the own public user identity under registration and the implicitly registered due to the received REGISTER request. Each public user identity is identified as either barred or non-barred; and,

b) all the service profile(s) corresponding to the public user identities being registered (explicitly or implicitly), including initial Filter Criteria(the initial Filter Criteria for the Registered and common parts is stored and the unregisterd part is retained for possible use later - in the case of the S-CSCF is retained if the user becomes unregistered);

NOTE 1: There might be more than one set of initial Filter Criteria received because some implicitly registered public user identities that are part of the same user"s subscription may belong to different service profiles.

6) bind to each non-barred registered public user identity all registered contact information including all header parameters contained in the Contact header and all associated URI parameters and store information for future use;

NOTE 2: There might be more then one contact information available for one public user identity.

NOTE 3: The barred public user identities are not bound to the contact information.

7) check whether a Path header was included in the REGISTER request and construct a list of preloaded Route headers from the list of entries in the Path header. The S-CSCF shall preserve the order of the preloaded Route headers and bind them to the contact information that was received in the REGISTER message;

NOTE 4: If this registration is a reregistration, then a list of pre-loaded Route headers will already exist. The new list replaces the old list.

8) determine the duration of the registration by checking the value of the Expires header in the received REGISTER request. The S-CSCF may reduce the duration of the registration due to local policy or send back a 423 (Interval Too Brief) response specifying the minimum allowed time for registration;

9) store the icid parameter received in the P-Charging-Vector header;

10) if an orig-ioi parameter is received in the P-Charging-Vector header, store the value of the received orig-ioi parameter;

NOTE 5: Any received orig-ioi parameter will be a type 1 orig-ioi. The type 1 orig-ioi identifies the network from which the request was sent.

11) create a 200 (OK) response for the REGISTER request, including:

a) the list of received Path headers;

b) a P-Associated-URI header containing the list of public user identities that are associated to the public user identity under registration. The first URI in the list of public user identities supplied by the HSS to the S-CSCF will indicate the default public user identity to be used by the S-CSCF. The public user identity indicated as the default public user identity must be an already registered public user identity. The S-CSCF shall place the default public user identity as a first entry in the list of URIs present in the P-Associated-URI header. The default public user identity will be used by the P-CSCF in conjunction with the procedures for the P-Asserted-Identity header, as described in subclause 5.2.6.3. The S-CSCF shall not add a barred public user identity to the list of URIs in the P-Associated-URI header;

c) a Service-Route header containing:

- the SIP URI identifying the S-CSCF containing an indication that requests routed via the service route (i.e. from the P-CSCF to the S-CSCF) are treated as for the mobile-originating case. This indication may e.g. be in a URI parameter, a character string in the user part of the URI or be a port number in the URI; and,

- if network topology hiding is required a SIP URI identifying an I-CSCF(THIG) as the topmost entry;

d) a P-Charging-Function-Addresses header containing the values received from the HSS if the P-CSCF is in the same network as the S-CSCF. It can be determined if the P-CSCF is in the same network as the S-CSCF by the contents of the P-Visited-Network-ID header field included in the REGISTER request;

e) a P-Charging-Vector header containing the orig-ioi parameter, if received in the REGISTER request and a type 1 term-ioi parameter. The S-CSCF shall set the type 1 term-ioi parameter to a value that identifies the sending network of the response and the orig-ioi parameter is set to the previously received value of orig-ioi; and

f) a Contact header listing all contact addresses for this public user identity.

NOTE 6: There might be other contact addresses available, that other UEs have registered for the same public user identity.

12) send the so created 200 (OK) response to the UE;

13) send a third-party REGISTER request, as described in subclause 5.4.1.7, to each AS that matches the Filter Criteria from the HSS for the REGISTER event; and,

NOTE 7: If this registration is a reregistration, the Filter Criteria already exists in the local data.

14) handle the user as registered for the duration indicated in the Expires header.

#### 5.4.1.2.3 Abnormal cases

In the case that the REGISTER request, that contains the authentication challenge response from the UE does not match with the expected REGISTER request (e.g. wrong Call-Id or authentication challenge response) and the request has the "integrity-protected" parameter in the Authorization header set to "yes", the S-CSCF shall:

- send a 403 (Forbidden) response to the UE. The S-CSCF shall consider this authentication attempt as failed. The S-CSCF shall not update the registration state of the subscriber.

NOTE 1: If the UE was registered before, it stays registered until the registration expiration time expires.

In the case that the REGISTER request, which was supposed to carry the response to the challenge, contains no authentication challenge response and no AUTS parameters indicating that the MAC parameter was invalid in the challenge, the S-CSCF shall:

- respond with a 403 (Forbidden) response to the UE. The S-CSCF shall not update the registration state of the subscriber.

NOTE 2: If the UE was registered before, it stays registered until the registration expiration time expires.

In the case that the REGISTER request from the UE containing an AUTS directive, indicating that the SQN was deemed to be out of range by the UE, the S-CSCF will fetch new authentication vectors from the HSS. In order to indicate a resynchronisation, the S-CSCF shall include the AUTS directive received from the UE and the stored RAND, when fetching the new authentication vectors. On receipt of the new authentication vectors from the HSS, the S-CSCF shall either:

- send a 401 (Unauthorized) response to initiate a further authentication attempt, using these new vectors; or

- respond with a 403 (Forbidden) response if the authentication attempt is to be abandoned. The S-CSCF shall not update the registration state of the subscriber.

NOTE 3: If the UE was registered before, it stays registered until the registration expiration time expires.

NOTE 4: Since the UE responds only to two consecutive invalid challenges, the S-CSCF will send a 401 (Unauthorized) response that contains a new challenge only twice.

NOTE 5: In the case of an AUTS directive being present in the REGISTER request, the response directive in the same REGISTER request will not be taken into account by the S-CSCF.

In the case that the expiration timer from the UE is too short to be accepted by the S-CSCF, the S-CSCF shall:

- reject the REGISTER request with a 423 (Interval Too Brief) response, containing a Min-Expires header with the minimum registration time the S-CSCF will accept.

On receiving a failure response to one of the third-party REGISTER requests, the S-CSCF may initiate network-initiated deregistration procedure based on the information in the Filter Criteria. If the Filter Criteria does not contain instruction to the S-CSCF regarding the failure of the contact to the AS, the S-CSCF shall not initiate network-initiated deregistration procedure.

In the case that the REGISTER request from the UE contains more than one SIP URIs as Contact header entries, the S-CSCF shall store the:

- entry with the highest "q" value;
- the entry in the contact header with the highest 'q'; or
- an entry decided by the S-CSCF based on local policy;

and include it in the 200 (OK) response.

NOTE 6: If the timer reg-await-auth expires, the S-CSCF will consider the authentication to have failed. If the public user identity was already registered, the S-CSCF will leave it as registered described in 3GPP TS 33.203 [19].

In the case that the S-CSCF receives a REGISTER request with the "integrity-protected" parameter in the Authorization header set to "yes", for which the public user identity received in the To header and the private user identity received in the Authorization header of the REGISTER request do not match to any registered user at this S-CSCF, the S-CSCF shall:

- respond with a 500 (Server Internal Error) response to the UE.

For any error response, the S-CSCF shall insert a P-Charging-Vector header containing the orig-ioi parameter, if received in the REGISTER request and a type 1 term-ioi parameter. The S-CSCF shall set the type 1 term-ioi parameter to a value that identifies the sending network of the response and the orig-ioi parameter is set to the previously received value of orig-ioi.

NOTE 7: Any previously received orig-ioi parameter will be a type 1 orig-ioi. The type 1 orig-ioi identifies the visited network of the registered user.

### 5.4.1.3 Authentication and reauthentication

Authentication and reauthentication is performed by the registration procedures as described in subclause 5.4.1.2.

### 5.4.1.4 User-initiated deregistration

When S-CSCF receives a REGISTER request with the Expires header field containing the value zero, the S-CSCF shall:

- check whether the "integrity-protected" parameter in the Authorization header field set to "yes", indicating that the REGISTER request was received integrity protected. The S-CSCF shall only proceed with the following steps if the "integrity-protected" parameter is set to "yes";
- release each multimedia session that includes this user, where the session was initiated by this UE with the public user identity found in the P-Asserted-Identity header field or with one of the implicitly registered public used identities by applying the steps listed in subclause 5.4.5.1.2;
- if this public used identity was registered only by this UE, deregister the public user identity found in the To header field together with the implicitly registered public user identities. Otherwise, the S-CSCF will only remove the contact address that was registered by this UE;
- send a third-party REGISTER request, as described in subclause 5.4.1.7, to each AS that matches the Filter Criteria from the HSS for the REGISTER event; and
- if this is a deregistration request for the only public user identity currently registered with its associated set of implicitly registered public user identities (i.e. no other is registered) and there are still active multimedia sessions that includes this user, where the session was initiated with the public user identity currently registered or with one of the implicitly registered public used identities, release each of these multimedia sessions by applying the steps listed in subclause 5.4.5.1.2.

If all public user identities of the UE are deregistered, then the S-CSCF may consider the UE and P-CSCF subscriptions to the reg event package cancelled (i.e. as if the UE had sent a SUBSCRIBE request with an Expires header containing a value of zero).

If the Authorization header of the REGISTER request did not contain an "integrity-protected" parameter, or the "integrity-protected" parameter was set to the value "no", the S-CSCF shall apply the procedures described in subclause 5.4.1.2.1.

On completion of the above procedures in this subclause and of the Cx Server Assignment procedure with the HSS, as described in 3GPP TS 29.228 [14], for one or more public user identities, the S-CSCF shall update or remove those public user identities, their registration state and the associated service profiles from the local data (based on operators' policy the S-CSCF can request of the HSS to either be kept or cleared as the S-CSCF allocated to this subscriber).

### 5.4.1.5 Network-initiated deregistration

NOTE 1: A network-initiated deregistration event that occurs at the S-CSCF may be received from the HSS or may be an internal event in the S-CSCF.

Prior to initiating the network-initiated deregistration for the only currently registered public user identity and its associated set of implicitly registered public user identities that have been registered with the same contact (i.e. no other public user identity is registered with this contact) while there are still active multimedia sessions belonging to this contact, the S-CSCF shall release only the multimedia sessions belonging to this contact as described in the following paragraph. The multimedia sessions for the same public user identity, if registered with another contact remain unchanged.

Prior to initiating the network-initiated deregistration while there are still active multimedia sessions that are associated with this user and contact, the S-CSCF shall release none, some or all of these multimedia sessions by applying the steps listed in subclause 5.4.5.1.2 under the following conditions:

- when the S-CSCF does not expect the UE to reregister (i.e. S-CSCF will set the event attribute within the <contact> element to "rejected" for the NOTIFY request, as described below), the S-CSCF shall release all sessions that are associated with the public user identities being deregistered, which includes the implicitly registered public user identities.

- when the S-CSCF expects the UE to reregister (i.e. S-CSCF will set the event attribute within the <contact> element to "deactivated" for the NOTIFY request, as described below), the S-CSCF shall only release sessions that currently include the user, where the session was initiated with the one of the public user identities being deregistered, which includes the implicitly registered public user identities.

When a network-initiated deregistration event occurs for one or more public user identities that are bound to one or more contacts, the S-CSCF shall send a NOTIFY request to all subscribers that have subscribed to the respective reg event package. For each NOTIFY request, the S-CSCF shall:

1) set the Request-URI and Route header to the saved route information during subscription;

2) set the Event header to the "reg" value;

3) in the body of the NOTIFY request, include as many <registration> elements as many public user identities the S-CSCF is aware of the user owns;

4) set the aor attribute within each <registration> element to one public user identity:

   a) set the <uri> sub-element inside the <contact> sub-element of each <registration> element to the contact address provided by the UE;

   b) if the public user identity:

      i) has been deregistered then:

         - set the state attribute within the <registration> element to "terminated";

         - set the state attribute within the <contact> element to "terminated"; and

         - set the event attribute within the <contact> element to "deactivated" if the S-CSCF expects the UE to reregister or "rejected" if the S-CSCF does not expect the UE to reregister; or

      ii) has been kept registered then:

         I) set the state attribute within the <registration> element to "active";

         II) set the state attribute within the <contact> element to:

- for the contact address to be removed set the state attribute within the <contact> element to "terminated", and event attribute element to "deactivated" if the S-CSCF expects the UE to reregister or "rejected" if the S-CSCF does not expect the UE to reregister; or

- for the contact address which remain unchanged, if any, leave the <contact> element unmodified; and

NOTE 2: There might be more than one contact information available for one public user identity. When deregistering this UE, the S-CSCF will only modify the <contact> elements that were originally registered by this UE using its private user identity. The <contact> elements of the same public user identitity, if registered by another UE using different private user identities remain unchanged.

5) add a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.260 [17].

The S-CSCF shall only include the non-barred public user identities in the NOTIFY request.

Also, the S-CSCF shall send a third-party REGISTER request, as described in subclause 5.4.1.7, to each AS that matches the Filter Criteria from the HSS as if a equivalent REGISTER request had been received from the user deregistering that public user identity, or combination of public user identities.

In case of the deregistration of the old contact information when the UE is roaming, registration is done in a new network and the previous registration has not expired, on completion of the above procedures, the S-CSCF shall remove the registration information related to the old contact from the local data.

Otherwise, on completion of the above procedures for one or more public user identities linked to the same private user identity, the S-CSCF shall deregister those public user identities and the associated implicitly registered public user identities. On completion of the Cx Server Assignment procedure with the HSS, as described in 3GPP TS 29.228 [14], the S-CSCF shall update or remove those public user identities linked to the same private user identity, their registration state and the associated service profiles from the local data (based on operators' policy the S-CSCF can request of the HSS to either be kept or cleared as the S-CSCF allocated to this subscriber). On the completion of the Cx Registration-Termination procedure with the HSS, as described in 3GPP TS 29.228 [14], the S-CSCF shall remove those public user identities, their registration state and the associated service profiles from the local data.

### 5.4.1.6 Network-initiated reauthentication

The S-CSCF may request a subscriber to reauthenticate at any time, based on a number of possible operator settable triggers as described in subclause 5.4.1.2.

If the S-CSCF is informed that a private user identity needs to be re-authenticated, the S-CSCF shall generate a NOTIFY request on all dialogs which have been established due to subscription to the reg event package of that user. For each NOTIFY request the S-CSCF shall:

1) set the Request-URI and Route header to the saved route information during subscription;

2) set the Event header to the "reg" value;

3) in the body of the NOTIFY request, include as many <registration> elements as many public user identities the S-CSCF is aware of the user owns:

   a) set the <uri> sub-element inside the <contact> sub-element of each <registration> element to the contact address provided by the UE;

   b) set the aor attribute within each <registration> element to one public user identity;

   c) set the state attribute within each <registration> element to "active";

   d) set the state attribute within each <contact> element to "active";

   e) set the event attribute within each <contact> element that was registered by this UE to "shortened"; and

   f) set the expiry attribute within each <contact> element that was registered by this UE to an operator defined value; and

NOTE 1: There might be more then one contact information available for one public user identity. The S-CSCF will only modify the <contact> elements that were originally registered by this UE using its private user identity. The S-CSCF will not modify the <contact> elements for the same public user identitity, if registered by another UE using different private user identity.

4) set a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.260 [17].

Afterwards the S-CSCF shall wait for the user to reauthenticate (see subclause 5.4.1.2).

NOTE 2: Network initiated re-authentication may occur due to internal processing within the S-CSCF.

The S-CSCF shall only include the non-barred public user identities in the NOTIFY request.

When generating the NOTIFY request, the S-CSCF shall shorten the validity of all registration lifetimes associated with this private user identity to an operator defined value that will allow the user to be re-authenticated.

### 5.4.1.7 Notification of Application Servers about registration status

During registration, the S-CSCF shall include a P-Access-Network-Info header (as received in the REGISTER request from the UE) in the 3rd-party REGISTER sent towards the ASs, if the AS is part of the trust domain. If the AS is not part of the trust domain, the S-CSCF shall not include any P-Access-Network-Info header. The S-CSCF shall not include a P-Access-Network-Info header in any responses to the REGISTER request.

If the registration procedure described in subclauses 5.4.1.2, 5.4.1.4 or 5.4.1.5 (as appropriate) was successful, the S-CSCF shall send a third-party REGISTER request to each AS with the following information:

a) the Request-URI, which shall contain the AS's SIP URI;

b) the From header, which shall contain the S-CSCF's SIP URI;

c) the To header, which shall contain a non-barred public user identity. It may be either a public user identity as contained in the REGISTER request received from the UE or one of the implicitly registered public user identities, as configured by the operator;

d) the Contact header, which shall contain the S-CSCF's SIP URI;

e) for initial registration and user-initiated reregistration (subclause 5.4.1.2), the Expires header, which shall contain the same value that the S-CSCF returned in the 200 (OK) response for the REGISTER request received form the UE;

f) for user-initiated deregistration (subclause 5.4.1.4) and network-initiated deregistration (subclause 5.4.1.5), the Expires header, which shall contain the value zero;

g) for initial registration and user-initiated reregistration (subclause 5.4.1.2), a message body, if there is Filter Criteria indicating the need to include HSS provided data for the REGISTER event (e.g. HSS may provide AS specific data to be included in the third-party REGISTER). If there is a service information XML element provided in the HSS Filter Criteria for an AS (see 3GPP TS 29.228 [14]), then the S-CSCF shall include it in the message body of the REGISTER request within the <service-info> XML element as described in subclause 7.6. For the messages including the IM CN subsystem XML body, the S-CSCF shall set the value of the Content-Type header to include the MIME type specified in subclause 7.6;

h) for initial registration and user-initiated reregistration, the P-Charging-Vector header, which shall contain the same icid parameter that the S-CSCF received in the original REGISTER request from the UE and add a type 3 orig-ioi parameter before the received orig-ioi parameter. The S-CSCF shall set the type 3 orig-ioi parameter to a value that identifies the sending network of the request. The S-CSCF shall not include the type 3 term-ioi parameter; and

i) for initial registration and user-initiated reregistration, a P-Charging-Function-Addresses header, which shall contain the values received from the HSS if the message is forwarded within the S-CSCF home network.

When the S-CSCF receives any response to a third-party REGISTER request, the S-CSCF shall store the value of the term-ioi parameter received in the P-Charging-Vector header, if present.

NOTE: Any received term-ioi parameter will be a type 3 term-ioi. The type 3 term-ioi identifies the service provider from which the response was sent.

If the S-CSCF fails to receive a SIP response or receives a 408 (Request Timeout) response or a 5xx response to a third-party REGISTER, the S-CSCF shall:

- if the default handling defined in the filter criteria indicates the value "SESSION_CONTINUED" as specified in 3GPP TS 29.228 [14] or no default handling is indicated, no further action is needed; and

- if the default handling defined in the filter criteria indicates the value "SESSION_TERMINATED" as specified in 3GPP TS 29.228 [14], the S-CSCF shall, for a currently registered public user identity, initiate the network-initiated deregistration as described in subclause 5.4.1.5.

## 5.4.2 Subscription and notification

### 5.4.2.1 Subscriptions to S-CSCF events

#### 5.4.2.1.1 Subscription to the event providing registration state

When an incoming SUBSCRIBE request addressed to S-CSCF arrives containing the Event header with the reg event package, the S-CSCF shall:

1) check if, based on the local policy, the request was generated by a subscriber who is authorised to subscribe to the registration state of this particular user. The authorized subscribers include:

   - all public user identities this particular user owns, that the S-CSCF is aware of, and which are not-barred;

   - all the entities identified by the Path header (i.e. the P-CSCF to which this user is attached to); and

   - all the ASs listed in the initial filter criteria and not belonging to third-party providers;

NOTE 1: The S-CSCF finds the identity for authentication of the subscription in the P-Asserted-Identity header received in the SUBSCRIBE request.

2) store the value of the orig-ioi parameter received in the P-Charging-Vector header if present; and

NOTE 2: Any received orig-ioi parameter will be a type 3 orig-ioi. The type 3 orig-ioi identifies the service provider from which the request was sent.

3) generate a 2xx response acknowledging the SUBSCRIBE request and indicating that the authorised subscription was successful as described in RFC 3680 [43]. The S-CSCF shall populate the header fields as follows:

   - an Expires header, set to either the same or a decreased value as the Expires header in SUBSCRIBE request; and

   - if the request originated from an ASs listed in the initial filter criteria, a P-Charging-Vector header containing the orig-ioi parameter, if received in the SUBSCRIBE request, and a type 3 term-ioi. The S-CSCF shall set the type 3 term-ioi parameter to a value that identifies the sending network of the response and the orig-ioi parameter is set to the previously received value of orig-ioi.

   The S-CSCF may set the Contact header to an identifier uniquely associated with the SUBSCRIBE request and generated within the S-CSCF, that may help the S-CSCF to correlate refreshes for the SUBSCRIBE.

NOTE 3: The S-CSCF could use such unique identifiers to distinguish between UEs, when two or more users, holding a shared subscription, register under the same public user identity.

Afterwards the S-CSCF shall perform the procedures for notification about registration state as described in subclause 5.4.2.1.2.

For any final response that is not a 2xx response, the S-CSCF shall insert a P-Charging-Vector header containing the orig-ioi parameter, if received in the SUBSCRIBE request and a type 3 term-ioi. The S-CSCF shall set the type 3 term-ioi parameter to a value that identifies the sending network of the response and the orig-ioi parameter is set to the previously received value of orig-ioi.

#### 5.4.2.1.2 Notification about registration state

For each NOTIFY request on all dialogs which have been established due to subscription to the reg event package of that user, the S-CSCF shall:

1) set the Request-URI and Route header to the saved route information during subscription;

2) set the Event header to the "reg" value;

3) in the body of the NOTIFY request, include as many <registration> elements as many public user identities the S-CSCF is aware of the user owns;

4) set the aor attribute within each <registration> element to one public user identity:

   a) set the <uri> sub-element inside each <contact> sub-element of the <registration> element to the contact address provided by the respective UE; and

   b) if the public user identity:

      I) has been deregistered (i.e. no active contact left) then:

         - set the state attribute within the <registration> element to "terminated";

         - set the state attribute within each <contact> element to "terminated"; and

         - set the event attribute within each <contact> element to "deactivated", "expired", "unregistered", "rejected" or "probation" according to RFC 3680 [43].

         If the public user identity has been deregistered and the deregistration has already been indicated in the NOTIFY request, and no new registration has occurred, its <registration> element shall not be included in the subsequent NOTIFY requests; or

      II) has been registered then:

         - set the <unknown-param> element to any additional header parameters contained in the contact header of the REGISTER request according to RFC 3680 [43];

         - set the state attribute within the <registration> element to "active", if not already set to "active", otherwise leave it unchanged; and either:

         - for the contact address to be registered: set the state attribute within the <contact> element to "active"; and set the event attribute within the <contact> element to "registered"; or

         - for the contact address which remain unchanged, if any, leave the <contact> element unmodified; or

      III) has been automatically registered, and have not been previously automatically registered:

         - set the <unknown-param> element to any additional header parameters contained in the contact header of the originsl REGISTER request according to RFC 3680 [43];

         - set the state attribute within the <registration> element to "active";

         - set the state attribute within the <contact> element to "active"; and

         - set the event attribute within the <contact> element to "created"; and

5) set the P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.260 [17]and a type 3 orig-ioi parameter. The S-CSCF shall set the type 3 orig-ioi parameter to a value that identifies the sending network of the request. The S-CSCF shall not include the type 3 term-ioi parameter.

The S-CSCF shall only include the non-barred public user identities in the NOTIFY request.

EXAMPLE: If sip:user1_public1@home1.net is registered, the public user identity sip:user1_public2@home1.net can automatically be registered. Therefore the entries in the body of the NOTIFY request look like:

```
<?xml version="1.0"?>
<reginfo xmlns="urn:ietf:params:xml:ns:reginfo"
```

```
            version="0" state="full">
  <registration aor="sip:user1_public1@home1.net" id="as9"
                state="active">
    <contact id="76" state="active" event="registered">
          <uri>sip:[5555::aaa:bbb:ccc:ddd]</uri>
          <unknown-param name="audio"/>
    </contact>
  </registration>
  <registration aor="sip:user1_public2@home1.net" id="as10"
                state="active">
    <contact id="86" state="active" event="created">
          <uri>sip:[5555::aaa:bbb:ccc:ddd]</uri>
          <unknown-param name="audio"/>
    </contact>
  </registration>
</reginfo>
```

When sending a final NOTIFY request with all <registration> element(s) having their state attribute set to "terminated" (i.e. all public user identities have been deregistered or expired), the S-CSCF shall also terminate the subscription to the registration event package by setting the Subscription-State header to the value of "terminated".

When all UE's contact addresses have been deregistered (i.e.there is no <contact> element set to "active" for this UE), the S-CSCF shall consider subscription to the reg event package belonging to the UE cancelled (i.e. as if the UE had sent a SUBSCRIBE request with an Expires header containing a value of zero).

The S-CSCF shall only include the non-barred public user identities in the NOTIFY request.

When the S-CSCF receives any response to the NOTIFY request, the S-CSCF shall store the value of the term-ioi parameter received in the P-Charging-Vector header, if present.

NOTE: Any received term-ioi parameter will be a type 3 term-ioi. The type 3 term-ioi identifies the service provider from which the response was sent.

## 5.4.3 General treatment for all dialogs and standalone transactions excluding requests terminated by the S-CSCF

### 5.4.3.1 Determination of mobile-originated or mobile-terminated case

Upon receipt of an initial request or a target refresh request or a stand-alone transaction, the S-CSCF shall:

- perform the procedures for the mobile-originating case as described in subclause 5.4.3.2 if the request makes use of the information for mobile-originating calls, which was added to the Service-Route header entry of the S-CSCF during registration (see subclause 5.4.1.2), e.g. the message is received at a certain port or the topmost Route header contains a specific user part or parameter; or,

- perform the procedures for the mobile-originating case as described in subclause 5.4.3.2 if the topmost Route header of the request contains the "orig" parameter. The S-CSCF shall remove the "orig" parameter from the topmost Route header; or,

- perform the procedures for the mobile-terminating case as described in subclause 5.4.3.3 if this information is not used by the request.

### 5.4.3.2 Requests initiated by the served user

When the S-CSCF receives from the served user or from a PSI an initial request for a dialog or a request for a standalone transaction, prior to forwarding the request, the S-CSCF shall:

Editor's Note: It needs to be stated, that the S-CSCF will only perform the following steps if the request was received from a trusted entity, e.g. an entity within the trust domain.

1) determine whether the request contains a barred public user identity in the P-Asserted-Identity header field of the request or not. In case the said header field contains a barred public user identity for the user, then the S-CSCF shall reject the request by generating a 403 (Forbidden) response. Otherwise, continue with the rest of the steps;

NOTE 1: If the P-Asserted-Identity header field contains a barred public user identity, then the message has been received, either directly or indirectly, from a non-compliant entity which should have had generated the content with a non-barred public user identity.

2) store the value of the orig-ioi parameter received in the P-Charging-Vector header if present, and remove it from any forwarded request;

NOTE 2: Any received orig-ioi parameter will be a type 3 orig-ioi. The type 3 orig-ioi identifies the service provider from which the request was sent (AS initiating a session on behalf of a user or a PSI);

3) check if an original dialog identifier that the S-CSCF previously placed in a Route header is present in the topmost Route header of the incoming request. If present, it indicates an association with an existing dialog, the request has been sent from an AS in response to a previously sent request;

4) remove its own SIP URI from the topmost Route header;

5) check whether the initial request matches the next unexecuted initial filter criteria based on a public user identity in the P-Asserted-Identity header in the priority order as described in 3GPP TS 23.218 [5], and if it does, the S-CSCF shall:

   a) insert the AS URI to be contacted into the Route header as the topmost entry followed by its own URI populated as specified in the subclause 5.4.3.4;

   b) if the AS is located outside the trust domain then the S-CSCF shall remove the P-Access-Network-Info header field and its values and the access-network-charging-info parameter in the P-Charging-Vector header from the request; if the AS is located within the trust domain, then the S-CSCF shall retain the P-Access-Network-Info header field and its values and the access-network-charging-info parameter in the P-Charging-Vector header in the request that is forwarded to the AS; and

   c) insert a type 3 orig-ioi parameter before the received orig-ioi parameters in the P-Charging-Vector header. The S-CSCF shall set the type 3 orig-ioi parameter to a value that identifies the sending network of the request. The S-CSCF shall not include the type 3 term-ioi parameter;

NOTE 3: Depending on the result of processing the filter criteria the S-CSCF might contact one or more AS(s) before processing the outgoing Request URI.

6) if there is no original dialog identifier present in the topmost Route header of the incoming request store the value of the icid parameter received in the P-Charging-Vector header and retain the icid parameter in the P-Charging-Vector header. Optionally, the S-CSCF may generate a new, globally unique icid and insert the new value in the icid parameter of the P-Charging-Vector header when forwarding the message. If the S-CSCF creates a new icid, then it is responsible for maintaining the two icid values in the subsequent messaging;

7) in step 5, if the initial request did not match the next unexecuted initial filter criteria (i.e. the request is not forwarded to an AS), insert a type 2 orig-ioi parameter into the P-Charging-Vector header. The S-CSCF shall set the type 2 orig-ioi parameter to a value that identifies the sending network. The S-CSCF shall not include the type 2 term-ioi parameter;

8) if there is no original dialog identifier present in the topmost Route header of the incoming request insert a P-Charging-Function-Addresses header populated with values received from the HSS if the message is forwarded within the S-CSCF home network, including towards AS;

9) if there is no original dialog identifier present in the topmost Route header of the incoming request and if the S-CSCF has knowledge that the SIP URI contained in the received P-Asserted-Identity header is an alias SIP URI for a tel URI, add a second P-Asserted-Identity header containing this tel-URI;

NOTE 4: The S-CSCF recognizes that a given SIP URI is an alias SIP URI of a tel URI, since they have the same service profile and belong to the same set of implicitly registered public user identities. If tel URI is shared URI so is the alias SIP URI.

Editors Note: The protocol support how to indicate which public user identities have the same service profile in Cx, Sh and Gm requires futher studies.

10) if the request is not forwarded to an AS and if the outgoing Request-URI is a tel URI, the S-CSCF shall translate the E.164 address (see RFC 3966 [22]) to a globally routeable SIP URI using an ENUM/DNS translation mechanism with the format specified in RFC 3761 24]. Databases aspects of ENUM are outside the scope of the

present document. If this translation fails, the request may be forwarded to a BGCF or any other appropriate entity (e.g a MRFC to play an announcement) in the originator's home network or the S-CSCF may send an appropriate SIP response to the originator. If the request is forwarded, the S-CSCF shall remove the access-network-charging-info parameter from the P-Charging-Vector header prior to forwarding the message. If the outgoing Request-URI is a pres URI or an im URI, the S-CSCF shall forward the request as specified in RFC 3861 [63]. In this case, the S-CSCF shall not modify the received Request-URI;

11) determine the destination address (e.g. DNS access) using the URI placed in the topmost Route header if present, otherwise based on the Request-URI. If the destination address is of an IP address type other than the IP address type used in the IM CN subsystem , then the S-CSCF shall forward the request to the IMS-ALG if the IM CN subsytem supports interworking to networks with different IP address type;

12) if network hiding is needed due to local policy, put the address of the I-CSCF(THIG) to the topmost route header;

13) in case of an initial request for a dialog originated from a served user, either:

- if the request is routed to an AS which is part of the trust domain, the S-CSCF can decide whether to record-route or not. The decision is configured in the S-CSCF using any information in the received request that may otherwise be used for the initial filter criteria. If the request is record-routed the S-CSCF shall create a Record-Route header containing its own SIP URI; or

- if the request is routed elsewhere, create a Record-Route header containing its own SIP URI;

NOTE 5: For requests originated from a PSI the S-CSCF can decide whether to record-route or not.

Editor's Note: It needs to be clarified how the S-CSCF decides whether to put its address into the Record-Route header in the case of handling a request that originates from a PSI. It might be part of the operators policy.

14) based on the destination user (Request-URI), remove the P-Access-Network-Info header and the access-network-charging-info parameter in the P-Charging-Vector header prior to forwarding the message;

15) route the request based on SIP routeing procedures; and

16) if the request is an INVITE request, save the Contact, Cseq and Record-Route header field values received in the request such that the S-CSCF is able to release the session if needed.

If the S-CSCF fails to receive a SIP response or receives a 408 (Request Timeout) response or a 5xx response from the AS, the S-CSCF shall:

- if the default handling defined in the filter criteria indicates the value "SESSION_CONTINUED" as specified in 3GPP TS 29.228 [14] or no default handling is indicated, execute the procedure from step 4; and

- if the default handling defined in the filter criteria indicates the value "SESSION_TERMINATED" as specified in 3GPP TS 29.228 [14], either forward the received response or send a 408 (Request Timeout) response or a 5xx response towards the served UE as appropriate (without verifying the matching of filter criteria of lower priority and without proceeding for further steps).

If the S-CSCF receives any final response from the AS, it shall forward the response towards the served UE (without verifying the matching of filter criteria of lower priority and without proceeding for further steps).

When the S-CSCF receives any response to the above request, the S-CSCF may:

1) apply any privacy required by RFC 3323 [33] and RFC 3325 [34] to the P-Asserted-Identity header.

NOTE 6: The P-Asserted-Identity header would normally only be expected in 1xx or 2xx responses.

NOTE 7: The optional procedure above is in addition to any procedure for the application of privacy at the edge of the trust domain specified by RFC 3325 [34].

When the S-CSCF receives any response to the above request containing a term-ioi parameter, the S-CSCF shall store the value of the received term-ioi parameter received in the P-Charging-Vector header, if present, and remove all received ioi parameters from the forwarded response if next hop is not an AS.

NOTE 8: Any received term-ioi parameter will be a type 2 term-ioi or type 3 term-ioi. The term-ioi parameter identifies the sending network of the response message

When the S-CSCF receives any response to the above request, and forwards it to AS, the S-CSCF shall insert a P-Charging-Vector header containing the orig-ioi parameter, if received in the request, and a type 3 term-ioi parameter in the response. The S-CSCF shall set the type 3 term-ioi parameter to a value that identifies the sending network of the response and the type 3 orig-ioi parameter is set to the previously received value of type 3 orig-ioi.

When the S-CSCF receives a 1xx or 2xx response to the initial request for a dialog, if the response corresponds to an INVITE request, the S-CSCF shall save the Contact and Record-Route header field values in the response in order to be able to release the session if needed.

When the S-CSCF, upon sending an initial INVITE request that includes an IPv6 address in the SDP offer (in "c=" parameter), receives an error response indicating that the the IP address type used in the IM CN subsystem is not supported, (e.g., the S-CSCF receives the 488 (Not Acceptable Here) with 301 Warning header indicating "incompatible network address format"), the S-CSCF shall either:

- fork the initial INVITE request to the IMS-ALG; or

- process the error response and forward it using the Via header.

When the S-CSCF receives from the served user a target refresh request for a dialog, prior to forwarding the request the S-CSCF shall:

1) remove its own URI from the topmost Route header;

2) create a Record-Route header containing its own SIP URI;

3) if the request is an INVITE request, save the Contact, Cseq and Record-Route header field values received in the request such that the S-CSCF is able to release the session if needed;

4) in case the request is routed towards the destination user (Request-URI) or in case the request is routed to an AS located outside the trust domain, remove the P-Access-Network-Info header and the access-network-charging-info parameter in the P-Charging-Vector header; and

5) route the request based on the topmost Route header.

When the S-CSCF receives a 1xx or 2xx response to the target refresh request for a dialog, if the response corresponds to an INVITE request, the S-CSCF shall save the Contact and Record-Route header field values in the response such that the S-CSCF is able to release the session if needed.

When the S-CSCF receives from the served user a subsequent request other than a target refresh request for a dialog, prior to forwarding the request the S-CSCF shall:

1) remove its own URI from the topmost Route header;

2) in case the request is routed towards the destination user (Request-URI) or in case the request is routed to an AS located outside the trust domain, remove the P-Access-Network-Info header and the access-network-charging-info parameter in the P-Charging-Vector header; and

3) route the request based on the topmost Route header.

#### 5.4.3.3 Requests terminated at the served user

When the S-CSCF receives, destined for a statically pre-configured PSI or a registered served user, an initial request for a dialog or a request for a standalone transaction, prior to forwarding the request, the S-CSCF shall:

1) check if an original dialog identifier that the S-CSCF previously placed in a Route header is present in the topmost Route header of the incoming request.

   - If present, it indicates an association with an existing dialog, the request has been sent from an AS in response to a previously sent request.

   - If not present, it indicates that the request is visiting the S-CSCF for the first time, and in this case the S-CSCF shall save the Request-URI from the request and in this case the S-CSCF shall determine whether the

request contains a barred public user identity in the Request-URI of the request or not. In case the Request URI contains a barred public user identity for the user, then the S-CSCF shall reject the request by generating a 404 (Not Found) response. Otherwise, the S-CSCF shall save the Request-URI from the request and continue with the rest of the steps;

2) remove its own URI from the topmost Route header;

3) if there was an original dialog identifier present in the topmost Route header of the incoming request check whether the Request-URI equals to the saved value of the Request-URI. If there is no match, then:

   a) if the request is an INVITE request, save the Contact, CSeq and Record-Route header field values received in the request such that the S-CSCF is able to release the session if needed; and

   b) forward the request based on the topmost Route header or if not available forward the request based on the Request-URI (routing based on Request-URI is specified in steps 10 through 14 from subclause 5.4.3.2) and skip the following steps;

4) check whether the initial request matches the next unexecuted initial filter criteria in the priority order and apply the filter criteria on the SIP method as described in 3GPP TS 23.218 [5] subclause 6.5. If there is a match, then the S-CSCF shall:

   - insert the AS URI to be contacted into the Route header as the topmost entry followed by its own URI populated as specified in the subclause 5.4.3.4; and

   - insert a type 3 orig-ioi parameter in the P-Charging-Vector header. The type 3 orig-ioi parameter identifies the sending network of the request message before the received orig-ioi. The S-CSCF shall not include the type 3 term-ioi parameter;

NOTE 1: Depending on the result of the previous process, the S-CSCF may contact one or more AS(s) before processing the outgoing Request-URI.

5) if there was no original dialog identifier present in the topmost Route header of the incoming request insert a P-Charging-Function-Addresses header field, if not present, populated with values received from the HSS if the message is forwarded within the S-CSCF home network, including towards AS;

6) if there was no original dialog identifier present in the topmost Route header of the incoming request store the value of the icid parameter received in the P-Charging-Vector header and retain the icid parameter in the P-Charging-Vector header;

7) if there was no original dialog identifier present in the topmost Route header of the incoming request store the value of the orig-ioi parameter received in the P-Charging-Vector header, if present, and remove all received ioi parameters from the forwarded request if next hop is not an AS;

NOTE 2: Any received orig-ioi parameter will be a type 2 orig-ioi or type 3 orig-ioi. The type 2 orig-ioi parameter identifies the sending network of the request message;

8) if necessary perform the caller preferences to callee capabilities matching according to RFC 3841 [56B];

9) in case there are no Route headers in the request, then determine, from the destination public user identity, the list of preloaded routes saved during registration or re-registration, as described in subclause 5.4.1.2. Furthermore, the S-CSCF shall:

   a) build the Route header field with the values determined in the previous step;

   b) determine, from the destination public user identity, the saved Contact URI where the user is reachable saved at registration or reregistration, as described in subclause 5.4.1.2. If there is more than one contact address saved for the destination public user identity, the S-CSCF shall:

      - if the fork directive in the Request Disposition header was set to "no-fork", the contact with the highest qvalue parameter shall be used when building the Request-URI. In case no qvalue parameters were provided, the S-CSCF shall decide locally what contact address to be used when building the Request-URI; otherwise

      - fork the request or perform sequential search based on the relative preference indicated by the qvalue parameter of the Contact header in the original REGISTER request, as described in RFC3261 [26]. In case no qvalue parameters were provided, then the S-CSCF determine the contact address to be used

when building the Request-URI as directed by the Request Disposition header as described in RFC 3841 [56B]. If the Request-Disposition header is not present, the S-CSCF shall decide locally whether to fork or perform sequential search among the contact addresses;

c) build a Request-URI with the contents of the saved Contact URI determined in the previous step; and

d) insert a P-Called-Party-ID SIP header field including the Request-URI received in the request;

10) if the request is an INVITE request, save the Contact, CSeq and Record-Route header field values received in the request such that the S-CSCF is able to release the session if needed;

11) optionally, apply any privacy required by RFC 3323 [33] and RFC 3325 [34] to the P-Asserted-Identity header ;

NOTE 3: The optional procedure above is in addition to any procedure for the application of privacy at the edge of the trust domain specified by RFC 3325 [34].

12) in case of an initial request for a dialog, either:

- if the request is routed to an AS which is part of the trust domain, the S-CSCF can decide whether to record-route or not. The decision is configured in the S-CSCF using any information in the received request that may otherwise be used for the initial filter criteria. If the request is record-routed the S-CSCF shall create a Record-Route header containing its own SIP URI; or

- if the request is routed elsewhere, create a Record-Route header containing its own SIP URI; and

13) forward the request based on the topmost Route header.

If the S-CSCF fails to receive a SIP response or receives a 408 (Request Timeout) response or a 5xx response from the AS, the S-CSCF shall:

- if the default handling defined in the filter criteria indicates the value "SESSION_CONTINUED" as specified in 3GPP TS 29.228 [14] or no default handling is indicated, execute the procedure from step 4; and

- if the default handling defined in the filter criteria indicates the value "SESSION_TERMINATED" as specified in 3GPP TS 29.228 [14], either forward the received response or send a 408 (Request Timeout) response or a 5xx response towards the originating UE as appropriate (without verifying the matching of filter criteria of lower priority and without proceeding for further steps).

If the S-CSCF receives any final response from the AS, it shall forward the response towards the originating UE (without verifying the matching of filter criteria of lower priority and without proceeding for further steps).

When the S-CSCF receives any response to the above request and forwards it to AS, the S-CSCF shall insert a P-Charging-Vector header containing the orig-ioi parameter, if received in the request, and a type 3 term-ioi parameter in the response. The S-CSCF shall set the type 3 term-ioi parameter to a value that identifies the sending network of the response and the orig-ioi parameter is set to the previously received value of orig-ioi.

NOTE 4: Any received term-ioi parameter will be a type 3 term-ioi. The term-ioi parameter identifies the service provider from which the response was sent.

When the S-CSCF receives, destined for an unregistered user, an initial request for a dialog or a request for a standalone transaction, the S-CSCF shall:

1) if the S-CSCF does not have the user profile, then initiate the S-CSCF Registration/deregistration notification with the purpose of downloading the relevant user profile (i.e. for unregistered user) and informing the HSS that the user is unregistered, but this S-CSCF will assess triggering of services for the unregistered user, as described in 3GPP TS 29.228 [14];

2) execute the procedures described in the steps 1, 2 and 3 in the above paragraph (when the S-CSCF receives, destined for the registered served user, an initial request for a dialog or a request for a standalone transaction); and

3) execute the procedure described in step 4, 5, 6, 7, 8, 10, 12 and 13 in the above paragraph (when the S-CSCF receives, destined for the registered served user, an initial request for a dialog or a request for a standalone transaction).

In case that no AS needs to be contacted, then S-CSCF shall return an appropriate unsuccessful SIP response. This response may be a 480 (Temporarily unavailable) and terminate these procedures.

When the S-CSCF receives a 1xx or 2xx response to the initial request for a dialog (whether the user is registered or not), it shall:

1) if the response corresponds to an INVITE request, save the Contact and Record-Route header field values in the response such that the S-CSCF is able to release the session if needed;

2) if the response did not match the next unexecuted initial filter criteria (i.e. the request is not forwarded to an AS), insert a type 2 term-ioi parameter in the P-Charging-Vector header of the outgoing response. The S-CSCF shall set the type 2 term-ioi parameter to a value that identifies the sending network of the response and the orig-ioi parameter is set to the previously received value of orig-ioi. Values of orig-ioi and term-ioi in the received response are removed;

3) in the case where the S-CSCF has knowledge that the SIP URI contained in the received P-Asserted-Identity header is an alias SIP URI for a tel URI, the S-CSCF shall add a second P-Asserted-Identity header containing this tel URI; and

4) in case the response is sent towards the originating user, the S-CSCF may remove the P-Access-Network-Info header based on local policy rules and the destination user (Request-URI).

When the S-CSCF receives a response to a request for a standalone transaction (whether the user is registered or not), in the case where the S-CSCF has knowledge that the SIP URI contained in the received P-Asserted-Identity header is an alias SIP URI for a tel URI, the S-CSCF shall add a second P-Asserted-Identity header containing this tel URI. In case the response is forwarded to an AS that is located within the trust domain, the S-CSCF shall retain the P-Access-Network-Info header and the access-network-charging-info parameter in the P-Charging-Vector header; otherwise, the S-CSCF shall remove the P-Access-Network-Info header and the access-network-charging-info parameter in the P-Charging-Vector header.

When the S-CSCF receives the 200 (OK) response for a standalone transaction request, the S-CSCF shall:

1) insert a P-Charging-Function-Addresses header populated with values received from the HSS if the message is forwarded within the S-CSCF home network, including towards an AS; and

2) if the response did not match the next unexecuted initial filter criteria (i.e. the request is not forwarded to an AS), insert a type 2 term-ioi parameter in the P-Charging-Vector header of the outgoing response. The S-CSCF shall set the type 2 term-ioi parameter to a value that identifies the sending network of the response and the type 2 orig-ioi parameter is set to the previously received value of orig-ioi.

When the S-CSCF receives, destined for a served user, a target refresh request for a dialog, prior to forwarding the request, the S-CSCF shall:

1) remove its own URI from the topmost Route header;

2) if the request is an INVITE request, save the Contact, Cseq and Record-Route header field values received in the request such that the S-CSCF is able to release the session if needed;

3) create a Record-Route header containing its own SIP URI; and

4) forward the request based on the topmost Route header.

When the S-CSCF receives a 1xx or 2xx response to the target refresh request for a dialog (whether the user is registered or not), the S-CSCF shall:

1) if the response corresponds to an INVITE request, save the Record-Route and Contact header field values in the response such that the S-CSCF is able to release the session if needed; and

2) in case the response is forwarded to an AS that is located within the trust domain, the S-CSCF shall retain the P-Access-Network-Info header and the access-network-charging-info parameter in the P-Charging-Vector header; otherwise, the S-CSCF shall remove the P-Access-Network-Info header and the access-network-charging-info parameter in the P-Charging-Vector header. ..

When the S-CSCF receives, destined for the served user, a subsequent request other than target refresh request for a dialog, prior to forwarding the request, the S-CSCF shall:

1) remove its own URI from the topmost Route header; and

2) forward the request based on the topmost Route header.

When the S-CSCF receives a response to a a subsequent request other than target refresh request for a dialog, in case the response is forwarded to an AS that is located within the trust domain, the S-CSCF shall retain the P-Access-Network-Info header and the access-network-charging-info parameter from the P-Charging-Vector header; otherwise, the S-CSCF shall remove the P-Access-Network-Info header and the access-network-charging-info parameter from the P-Charging-Vector header.

#### 5.4.3.4 Original dialog identifier

The original dialog identifier is an implementation specific token that the S-CSCF encodes into the own S-CSCF URI in a Route header, prior to forwarding the request to an AS. This is possible because the S-CSCF is the only entity that creates and consumes the value.

The token identifies the original dialog of the request, so in case an AS acting as a B2BUA changes the dialog, the S-CSCF is able to identify the original dialog when the request returns to the S-CSCF. The token can be encoded in different ways, such as e.g., a character string in the user-part of the S-CSCF URI, a parameter in the S-CSCF URI or port number in the S-CSCF URI.

The S-CSCF shall ensure that the value chosen is unique so that the S-CSCF may recognize the value when received in a subsequent message and make the proper association between related dialogs that pass through an AS.

#### 5.4.3.5 Void

### 5.4.4 Call initiation

#### 5.4.4.1 Initial INVITE

When the S-CSCF receives an INVITE request, either from the served user or destined to the served user, the S-CSCF may require the periodic refreshment of the session to avoid hung states in the S-CSCF. If the S-CSCF requires the session to be refreshed, it shall apply the procedures described in RFC 4028[58] clause 8.

NOTE 1: Requesting the session to be refreshed requires support by at least one of the UEs. This functionality cannot automatically be granted, i.e. at least one of the involved UEs needs to support it.

When the S-CSCF receives an initial INVITE request destined for the served user, it shall either:

a) examine the SDP offer (the "c=" parameter) to detect if it contains an IP address type that is not supported by the IM CN subsystem; or

b) process the initial INVITE request without examining the SDP.

NOTE 2: If the SDP offer contained an IP address type that is not supported by the IM CN subsystem, the S-CSCF will receive the 488 (Not Acceptable Here) response with 301 Warning header indicating "incompatible network address format".

Subsequently, when the S-CSCF detects that the SDP offer contained an IP address type that is not supported by the IM CN subsystem (i.e., either case a) or b)), the S-CSCF shall either:

- return a 305 (Use Proxy) response to the I-CSCF with the Contact field containing the SIP URI of the IMS-ALG, or

- forward the initial INVITE request to the IMS-ALG. When forwarding the initial INVITE request, the S-CSCF shall not insert its SIP URI into the Record-Route header.

#### 5.4.4.2 Subsequent requests

##### 5.4.4.2.1 Mobile-originating case

When the S-CSCF receives any 1xx or 2xx response, the S-CSCF shall insert a P-Charging-Function-Addresses header populated with values received from the HSS if the message is forwarded within the S-CSCF home network, including towards AS.

When the S-CSCF receives the request containing the access-network-charging-info parameter in the P-Charging-Vector, the S-CSCF shall store the access-network-charging-info parameter from the P-Charging-Vector header. The S-CSCF shall retain access-network-charging-info parameter in the P-Charging-Vector header when the request is forwarded to an AS. However, the S-CSCF shall not include the access-network-charging-info parameter in the P-Charging-Vector header when the request is forwarded outside the home network of the S-CSCF.

When the S-CSCF receives any request or response (excluding ACK requests and CANCEL requests and responses) related to a mobile-originated dialog or standalone transaction, the S-CSCF may insert previously saved values into P-Charging-Vector and P-Charging-Function-Addresses headers before forwarding the message within the S-CSCF home network, including towards AS.

##### 5.4.4.2.2 Mobile-terminating case

When the S-CSCF receives the any 1xx or 2xx response, the S-CSCF shall insert a P-Charging-Function-Addresses header populated with values received from the HSS if the message is forwarded within the S-CSCF home network, including towards AS.

When the S-CSCF receives 180 (Ringing) or 200 (OK) (to INVITE) responses containing the access-network-charging-info parameter in the P-Charging-Vector, the S-CSCF shall store the access-network-charging-info parameter from the P-Charging-Vector header. The S-CSCF shall retain the access-network-charging-info parameter in the P-Charging-Vector header when the response is forwarded to an AS. However, the S-CSCF shall not include the access-network-charging-info parameter in the P-Charging-Vector header when the response is forwarded outside the home network of the S-CSCF.

When the S-CSCF receives any request or response (excluding ACK requests and CANCEL requests and responses) related to a mobile- terminated dialog or standalone transaction, the S-CSCF may insert previously saved values into P-Charging-Vector and P-Charging-Function-Addresses headers before forwarding the message within the S-CSCF home network, including towards AS.

### 5.4.5 Call release

#### 5.4.5.1 S-CSCF-initiated session release

##### 5.4.5.1.1 Cancellation of a session currently being established

Upon receipt of an network internal indication to release a session which is currently being established, the S-CSCF shall cancel the related dialogs by sending the CANCEL request according to the procedures described in RFC 3261 [26].

##### 5.4.5.1.2 Release of an existing session

Upon receipt of a network internal indication to release an existing multimedia session, the S-CSCF shall:

1) generate a first BYE request for the called user based on the information saved for the related dialog, including:

   - a Request-URI, set to the stored Contact header provided by the called user;
   - a To header, set to the To header value as received in the 200 OK response for the initial INVITE request;
   - a From header, set to the From header value as received in the initial INVITE request;
   - a Call-ID header, set to the Call-Id header value as received in the initial INVITE request;

- a CSeq header, set to the CSeq value that was stored for the direction from the calling to the called user, incremented by one;
- a Route header, set to the routeing information towards the called user as stored for the dialog;
- further headers, based on local policy or the requested session release reason.

2) generate a second BYE request for the calling user based on the information saved for the related dialog, including:
   - a Request-URI, set to the stored Contact header provided by the calling user;
   - a To header, set to the From header value as received in the initial INVITE request;
   - a From header, set to the To header value as received in the 200 OK response for the initial INVITE request;
   - a Call-ID header, set to the Call-Id header value as received in the initial INVITE request;
   - a CSeq header, set to the CSeq value that was stored for the direction from the called to the calling user, incremented by one – if no CSeq value was stored for that session it shall generate and apply a random number within the valid range for CSeqs;
   - a Route header, set to the routeing information towards the calling user as stored for the dialog;
   - further headers, based on local policy or the requested session release reason.
3) if the S-CSCF serves the calling user, treat the first BYE request as if received directly from the calling user, i.e. send it to internal service control and based on the outcome further on towards the called user;
4) if the S-CSCF serves the calling user, send the second BYE request directly to the calling user.
5) if the S-CSCF serves the called user, send the first BYE request directly to the called user;
6) if the S-CSCF serves the called user, treat the second BYE request as if received directly from the called user, i.e. shall send it to internal service control and based on the outcome further on towards to the calling user.

Upon receipt of the 2xx responses for both BYE requests, the S-CSCF shall release all information related to the dialog and the related multimedia session.

#### 5.4.5.1.2A Release of the existing dialogs due to registration expiration

When the registration lifetime of the only public user identity currently registered with its associated set of implicitly registered public user identities (i.e. no other is registered) expires while there are still active multimedia sessions that includes this user, where the session was initiated with the public user identity currently registered or with one of the implicitly registered public used identities, the S-CSCF shall release each of these multimedia sessions by applying the steps listed in the subclause 5.4.5.1.2.

#### 5.4.5.1.3 Abnormal cases

Upon receipt of a request on a dialog for which the S-CSCF initiated session release, the S-CSCF shall terminate the received request and answer it with a 481 (Call/Transaction Does Not Exist) response.

### 5.4.5.2 Session release initiated by any other entity

Upon receipt of a 2xx response for a BYE request matching an existing dialog, the S-CSCF shall delete all the stored information related to the dialog.

### 5.4.5.3 Session expiration

If the S-CSCF requested the session to be refreshed periodically, and the S-CSCF got the indication that the session will be refreshed, when the session timer expires, the S-CSCF shall delete all the stored information related to the dialog.

### 5.4.6 Call-related requests

#### 5.4.6.1 ReINVITE

##### 5.4.6.1.1 Determination of served user

Void.

##### 5.4.6.1.2 Mobile-originating case

For a reINVITE request or UPDATE request from the UE within the same dialog, the S-CSCF shall store the updated access-network-charging-info parameter from P-Charging-Vector header in the received SIP request. The S-CSCF shall retain the access-network-charging-info parameter in the P-Charging-Vector header when the request is forwarded to an AS. However, the S-CSCF shall not include the access-network-charging-info parameter in the P-Charging-Vector header when the request is forwarded outside the home network of the S-CSCF.

For a reINVITE request from the UE, if the request is to be forwarded to an AS that is located within the trust domain, the S-CSCF shall retain the P-Access-Network-Info header and the access-network-charging-info parameter from the P-Charging-Vector header; otherwise, the S-CSCF shall remove the P-Access-Network-Info header and the access-network-charging-info parameter from the P-Charging-Vector header.

##### 5.4.6.1.3 Mobile-terminating case

For a reINVITE request or UPDATE request destined towards the UE within the same dialog, when the S-CSCF receives the 200 (OK) response (to the INVITE request or UPDATE request), the S-CSCF shall store the updated access-network-charging-info parameter from the P-Charging-Vector header. The S-CSCF shall retain the access-network-charging-info parameter in the P-Charging-Vector header when the response is forwarded to the AS. However, the S-CSCF shall include the access-network-charging-info parameter in the P-Charging-Vector header when the 200 (OK) response is forwarded outside the home network of the S-CSCF.

For any SIP response to an INVITE request, if the response is to be forwarded to an AS that is located within the trust domain, the S-CSCF shall retain the P-Access-Network-Info header and the access-network-charging-info parameter from the P-Charging-Vector header; otherwise, the S-CSCF shall remove the P-Access-Network-Info header and the access-network-charging-info parameter from the P-Charging-Vector header.

### 5.4.7 Void

## 5.5 Procedures at the MGCF

### 5.5.1 General

The MGCF, although acting as a UA, does not initiate any registration of its associated addresses. These are assumed to be known by peer-to-peer arrangements within the IM CN subsystem. Therefore table A.4/1 and dependencies on that major capability shall not apply.

The use of the Path and Service-Route headers shall not be supported by the MGCF.

When the MGCF sends any request or response related to a dialog, the MGCF may insert previously saved values into P-Charging-Vector and P-Charging-Function-Addresses headers before sending the message.

### 5.5.2 Subscription and notification

Void.

## 5.5.3 Call initiation

### 5.5.3.1 Initial INVITE

#### 5.5.3.1.1 Calls originated from circuit-switched networks

When the MGCF receives an indication of an incoming call from a circuit-switched network, the MGCF shall:

1) generate and send an INVITE request to I-CSCF:

   - set the Request-URI to the "tel" format using an E.164 address;

   - set the Supported header to "100rel" (see RFC 3312 [30] as updated by RFC 4028 [64]));

   - include an P-Asserted-Identity header, depending on corresponding information in the circuit-switched network;

   - create a new, globally unique value for the icid parameter and insert it into the P-Charging-Vector header; and

   - insert a type 2 orig-ioi parameter into the P-Charging-Vector header. The type 2 orig-ioi parameter shall be set to a value that identifies the sending network in which the MGCF resides and the type 2 term-ioi parameter shall not be included.

When the MGCF receives a 1xx or 2xx response to an initial request for a dialog, the MGCF shall store the value of the received term-ioi parameter received in the P-Charging-Vector header, if present.

NOTE: Any received term-ioi parameter will be a type 2 term-ioi. The type 2 term-ioi parameter identifies the sending network of the response message.

#### 5.5.3.1.2 Calls terminating in circuit-switched networks

When the MGCF receives an initial INVITE request with Supported header indicating "100rel", the MGCF shall:

1) store the value of the orig-ioi parameter received in the P-Charging-Vector header, if present;

NOTE: Any received orig-ioi parameter will be a type 2 orig-ioi. The type 2 orig-ioi parameter identifies the sending network of the request message.

2) send a 100 (Trying) response;

3) after a matching codec is found or no codec is required at the MGW, send 183 "Session Progress" response:

   - set the Require header to the value of "100rel";

   - store the values received in the P-Charging-Function-Addresses header;

   - store the value of the icid parameter received in the P-Charging-Vector header; and

   - insert a P-Charging-Vector header containing the orig-ioi parameter, if received in the initial INVITE request and a type 2 term-ioi. The MGCF shall set the type 2 term-ioi parameter to a value that identifies the network in which the MGCF resides and the orig-ioi parameter is set to the previously received value of orig-ioi.

If a codec is required and the MGCF does not find an available matching codec at the MGW for the received initial INVITE request, the MGCF shall:

- send 503 (Service Unavailable) response if the type of codec was acceptable but none were available; or

- send 488 (Not Acceptable Here) response if the type of codec was not supported, and may include SDP in the message body to indicate the codecs supported by the MGCF/MGW.

#### 5.5.3.2 Subsequent requests

##### 5.5.3.2.1 Calls originating in circuit-switched networks

When the MGCF receives 183 response to an INVITE request, the MGCF shall:

- store the values received in the P-Charging-Function-Addresses header.

The MGCF shall send an UPDATE request when the following conditions are fulfilled:

- conditions as specified in 3GPP TS 29.153 [11B]; and
- the MGCF receives 200 (OK) response to a PRACK request

##### 5.5.3.2.2 Calls terminating in circuit-switched networks

When the MGCF receives an indication of a ringing for the called party of outgoing call to a circuit-switched network, the MGCF shall:

- send 180 (Ringing) response to the UE.

When the MGCF receives an indication of answer for the called party of outgoing call to a circuit-switched network, the MGCF shall:

- send 200 (OK) response to the UE. The 200 (OK) response shall include an P-Asserted-Identity header if corresponding information is received from the circuit-switched network.

### 5.5.4 Call release

#### 5.5.4.1 Call release initiated by a circuit-switched network

When the MGCF receives an indication of call release from a circuit-switched network, the MGCF shall:

- send a BYE request to the UE.

#### 5.5.4.2 IM CN subsystem initiated call release

NOTE: The release of a call towards the circuit-switched network additionally requires signaling procedures other than SIP in the MGCF that are outside the scope of this document.

#### 5.5.4.3 MGW-initiated call release

When the MGCF receives an indication from the MGW that the bearer was lost, the MGCF shall:

- send a BYE request towards the UE; and
- may include Error-Info header witha pointer to additional information indicating that bearer was lost.

### 5.5.5 Call-related requests

#### 5.5.5.1 ReINVITE

##### 5.5.5.1.1 Calls originating from circuit-switched networks

Void.

##### 5.5.5.1.2 Calls terminating in circuit-switched networks

When the MGCF receives a reINVITE request for hold/resume operation, the MGCF shall:

- send 100 (Trying) response;
- after performing interaction with MGW to hold/resume the media flow, send 200 (OK) response.

### 5.5.6 Further initial requests

When the MGCF responds to an OPTIONS request with a 200 (OK) response, the MGCF may include a message body with an indication of the DTMF capabilities and supported codecs of the MGCF/MGW.

NOTE: The detailed interface for requesting MGCF/MGW capabilities is not specified in this version of the document. Other solutions may be used in the interim.

## 5.6 Procedures at the BGCF

### 5.6.1 General

The use of the Path and Service-Route headers shall not be supported by the BGCF.

When the BGCF receives any request or response (excluding ACK requests and CANCEL requests and responses) related to a dialog or standalone transaction, the BGCF may insert previously saved values into P-Charging-Vector and P-Charging-Function-Addresses headers before forwarding the message.

### 5.6.2 Session initiation transaction

When the BGCF receives an INVITE request, the BGCF shall forward the request either to an MGCF within its own network, or to another network containing an MGCF. The BGCF need not Record-Route the INVITE request. While the next entity may be a MGCF acting as a UA, the BGCF shall not apply the procedures of RFC 3323 [33] relating to privacy. The BGCF shall store the values received in the P-Charging-Function-Addresses header. The BGCF shall store the value of the icid parameter received in the P-Charging-Vector header and retain the icid parameter in the P-Charging-Vector header.

NOTE 1: The means by which the decision is made to forward to an MGCF or to another network is outside the scope of the present document, but may be by means of a lookup to an external database, or may be by data held internally to the BGCF.

When the BGCF receives an INVITE request, if the BGCF inserts its own Record-Route header, the BGCF may require the periodic refreshment of the session to avoid hung states in the BGCF. If the BGCF requires the session to be refreshed, it shall apply the procedures described in RFC 4028[58] clause 8.

NOTE 2: Requesting the session to be refreshed requires support by at least one of the UEs. This functionality cannot automatically be granted, i.e. at least one of the involved UEs needs to support it.

## 5.7 Procedures at the Application Server (AS)

### 5.7.1 Common Application Server (AS) procedures

#### 5.7.1.1 Notification about registration status

The AS may support the REGISTER method in order to discover the registration status of the user. If a REGISTER request arrives containing information about the user's registration status and the AS supports the REGISTER method, the AS shall store the Expires parameter from the request and generate a 200 (OK) response or an appropriate failure response. For the success case, the 200 (OK) response shall contain Expires value equal to the value received in the REGISTER request. The AS shall store the values received in P-Charging-Function-Addresses header. Also, the AS shall store the values of the icid parameter and orig-ioi parameter if present in the P-Charging-Vector header from the REGISTER request. The AS shall insert a P-Charging-Vector header containing the orig-ioi parameters, if received in the REGISTER request and a type 3 term-ioi parameter in the response to REGISTER. The AS shall set the type 3 term-ioi parameter to a value that identifies the service provider from which the response is sent and the orig-ioi parameter is set to the previously received value of orig-ioi.

Upon receipt of a third-party REGISTER request, the AS may subscribe to the reg event package for the public user identity registered at the users registrar (S-CSCF) as described in RFC 3680 [43].

On sending a SUBSCRIBE request, the AS shall populate the header fields as follows:

a) a Request URI set to the resource to which the AS wants to be subscribed to, i.e. to a SIP URI that contains the public user identity of the user that was received in the To header field of the third-party REGISTER request;

b) a From header field set to the AS"s SIP URI;

c) a To header field, set to a SIP URI that contains the public user identity of the user that was received in the To header field of the third-party REGISTER request;

d) an Event header set to the "reg" event package;

e) a P-Asserted-Identity header field set to the SIP URI of the AS; and

NOTE 1: The S-CSCF expects the SIP URI used in the P-Asserted-Identity header to correspond to the SIP URI, which identified this AS in the initial filter criteria of the user to whose registration state the AS subscribes to.

f) a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.260 [17] and a type 3 orig-ioi parameter. The type 3 orig-ioi identifies the service provider from which the request is sent. The AS shall not include the type 3 term-ioi parameter.

Upon receipt of a 2xx response to the SUBSCRIBE request, the AS shall store the information for the so established dialog and the expiration time as indicated in the Expires header of the received response.

Upon receipt of any response, the AS shall store the value of the term-ioi parameters received in the P-Charging-Vector header if present.

NOTE 2: Any received term-ioi parameters will be any type term-ioi but includes the adjacent network term ioi in frst position. The first type 3 term-ioi identifies the network operator from which the response was originated for a release 5 S-CSCF and the network operator from which the request was sent otherwise.

NOTE 3: Upon receipt of a NOTIFY request with all <registration> element(s) having their state attribute set to "terminated" (i.e. all public user identities are deregistered) and the Subscription-State header set to "terminated", the AS considers the subscription to the reg event package terminated, i.e. as if the AS had sent a SUBSCRIBE request with an Expires header containing a value of zero.

Upon receipt of a NOTIFY request, the AS shall store the value of the orig-ioi parameters if present in the P-Charging-Vector header. The AS shall insert a P-Charging-Vector header in the response to the NOTIFY rquest containing the orig-ioi parameter, if received in the NOTIFY request and a type 3 term-ioi. The AS shall set the type 3 term-ioi parameter to a value that identifies the service provider from which the response is sent and the orig-ioi parameter is set to the previously received value of orig-ioi.

### 5.7.1.2 Extracting charging correlation information

When an AS receives an initial request for a dialog or a request (excluding ACK requests and CANCEL requests and responses) for a standalone transaction, the AS shall store the values received in the P-Charging-Vector header, e.g. orig-ioi parameters, if present, and icid parameter, and retain the P-Charging-Vector header in the message. The AS shall store the values received in the P-Charging-Function-Addresses header and retain the P-Charging-Function-Addresses header in the message.

When an AS sends any request or response related to a dialog or standalone transaction, the AS may insert previously saved values into the P-Charging-Vector and P-Charging-Function-Addresses headers before sending the message.

### 5.7.1.3 Access-Network-Info

The AS may receive in any request or response (excluding ACK requests and CANCEL requests and responses) information about the served user access network. This information is contained in the P-Access-Network-Info header. The AS can use the header to provide an appropriate service to the user.

### 5.7.1.4 User identify verification at the AS

The procedures at the AS to accomplish user identity verification are described with the help of figure 5-1.

When the AS receives a SIP initial or standalone request, excluding REGISTER request, that does not contain credentials, the AS shall:

Editor's Note: it is not clear what are the mechanisms available to transport the credentials. These mechanisms can include, among others, P-Asserted-Identity, Authorization header, digital signatures, S/MIME body, etc.

a) if a Privacy header is present in the initial or standalone request and the Privacy header value is set to "id" or "user", then the user and the request are considered as anonymous, and no further actions are required. The AS shall consider the request as authenticated;

b) if there is no Privacy header present in the initial or standalone request, or if the Privacy header contains a value other than "id" or "user", then the AS shall check for the presence of a P-Asserted-Identity header in the initial or standalone request. Two cases exists:

   i) the initial or standalone request contains a P-Asserted-Identity header. This is typically the case when the user is located inside a trusted domain as defined by subclause 4.4. In this case, the AS is aware of the identity of the user and no extra actions are needed. The AS shall consider the request as authenticated.

   ii) the initial or standalone request does not contain a P-Asserted-Identity header. This is typically the case when the user is located outside a trusted domain as defined by subclause 4.4. In this case, the AS does not have a verified identity of the user. The AS shall check the From header of the initial or standalone request. If the From header value in the initial or standalone request is set to "Anonymous", then the user and the request are considered as anonymous and no further actions are required. If the From header value does not indicate anonymity, then the AS shall challenge the user by issuing a 401 (Unauthorized) response including a challenge as per procedures described in RFC 3261 [26].

When the AS receives a SIP initial or standalone request that contains credentials but it does not contain a P-Asserted-Identity header the AS shall check the correctness of the credentials as follows:

a) If the credentials are correct, then the AS shall consider the identity of the user verified, and the AS shall consider the request as authenticated;

b) If the credentials are not correct, the AS may either rechallenge the user by issuing a 401 (Unauthorized) response including a challenge as per procedures described in RFC 3261 [26] (up to a predetermined maximum number of times predefined in the AS configuration data), or consider the user as anonymous. If the user is considered anonymous, the PS shall consider the request as authenticated.

Editor's Note: It needs to be investigated whether the *maximum number of times predefined in the AS configuration data* creates a potential denial of service attack, as it requires the AS to keep states between different authentications trials.

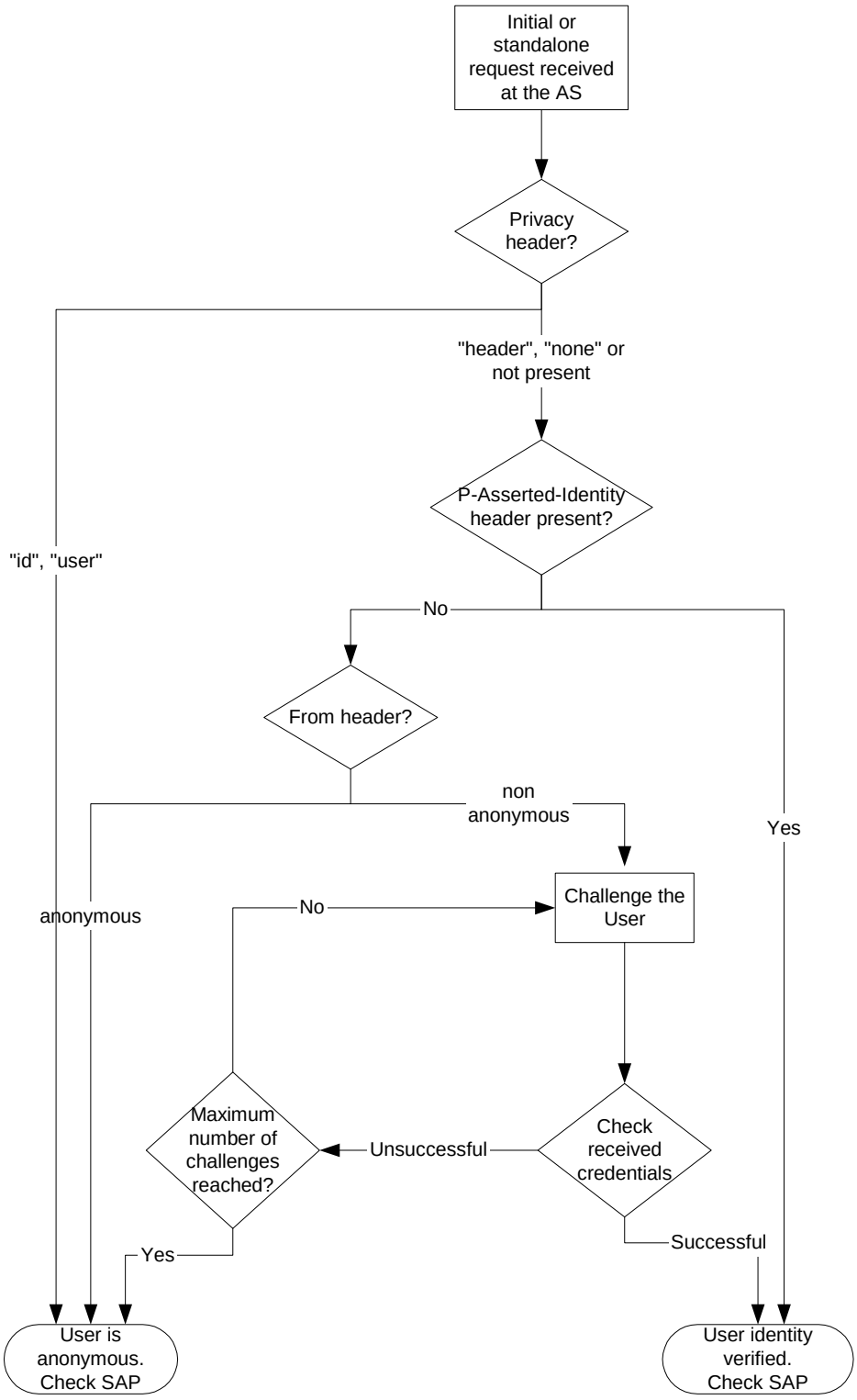



**Figure 5-1: User identity verification flow at the AS**

#### 5.7.1.5 Request authorization

Once the AS have tried to verify the identity of the user, the AS either has a verified identity of the user or it considers the user as anonymous.

If the user is considered anonymous, the AS shall check whether the authorization policy defined for this request allows anonymous requests. If anonymous requests are allowed, then the AS can proceed with the requested functionality, otherwise, the AS shall not proceed with the requested functionality.

If the user is identified by an identity, the AS shall apply the authorization policy related to the requested functionality to detect whether the particular user is allowed to request the functionality. The authorization policy may require a verified identity of a user.

If the request is authorized then the AS shall continue with the procedures as defined for that request.

If the request is not authorized, the AS shall either:

- reject the request according to the procedures defined for that request e.g., by issuing a 403 (Forbidden) response; or
- send a 2xx final response if the authorization policy requires to deny the requested functionality, whilst appearing to the user as if the request has been granted.

#### 5.7.1.6 Event notification throttling

If the AS has a local configuration information limiting the rate at which notification generation is allowed, then the AS shall take that information into account. Such local configuration information could be e.g. the shortest time period between issuing consecutive NOTIFY requests.

### 5.7.2 Application Server (AS) acting as terminating UA, or redirect server

When acting as a terminating UA the AS shall behave as defined for a UE in subclause 5.1.4, with the exceptions identified in this subclause.

The AS, although acting as a UA, does not initiate any registration of its associated addresses. These are assumed to be known by peer-to-peer arrangements within the IM CN subsystem.

An AS acting as redirect server shall propagate any received IM CN subsystem XML message body in the redirected message.

When an AS acting as a terminating UA generates a subsequent request that does not relate to an INVITE dialog, the AS shall insert a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.260 [17].

When the AS acting as terminating UA receives an initial request for a dialog or a request for a standalone transaction, it shall store the value of the orig-ioi parameters received in the P-Charging-Vector header if present.

NOTE: Any received orig-ioi parameters will be any type orig-ioi but includes the adjacent network term ioi in frst position. The first orig-ioi identifies the network operator from which the request was originated for a release 5 S-CSCF and the network operator from which the request was sent otherwise.

When the AS acting as terminating UA generates a response to an initial request for a dialog or a request for a standalone transaction, it shall insert a P-Charging-Vector header containing the orig-ioi parameters, if received in the request and a type 3 term-ioi. The AS shall set the type 3 term-ioi parameter to a value that identifies the service provider from which the response is sent and the orig-ioi parameter is set to the previously received value of orig-ioi.

### 5.7.3 Application Server (AS) acting as originating UA

When acting as an originating UA the AS shall behave as defined for a UE in subclause 5.1.3, with the exceptions identified in this subclause.

The AS, although acting as a UA, does not initiate any registration of its associated addresses. These are assumed to be known by peer-to-peer arrangements within the IM CN subsystem.

When an AS acting as an originating UA generates an initial request for a dialog or a request for a standalone transaction, the AS shall insert a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.260 [17] and a type 3 orig-ioi. The AS shall set the type 3 orig-ioi parameter to a value that identifies the service provider from which the request is sent. The AS shall not include the type 3 term-ioi parameter. The AS may retrieve CCF and/or ECF addresses from HSS on Sh interface.

When the AS acting as an originating UA receives any response to an initial request for a dialog or a request for a standalone transaction, it shall store the value of the term-ioi parameters received in the P-Charging-Vector header if present.

NOTE 1: Any received term-ioi parameter will be a type 3 term-ioi. The type 3 term-ioi identifies the network operator from which the response was sent.

When an AS acting as an originating UA generates a subsequent request that does not relate to an INVITE dialog, the AS shall insert a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.260 [17].

The AS shall extract charging function addresses from any P-Charging-Function-Addresses header that is received in any 1xx or 2xx responses to the requests.

The AS may also indicate that the proxies should not fork the INVITE request by including a "no-fork" directive within the Request-Disposition header in the initial INVITE request as described in RFC 3841 [56B].

When sending an initial request on behalf of a PSI that is hosted by the AS, the AS shall insert a Route header pointing to an S-CSCF of the home network of the PSI, if:

- the AS is not able to resolve the next hop address by itself; or
- the operator policy requires it.

NOTE 2: The address of the S-CSCF may be obtained by querying the HSS on the Sh interface or from static configuration.

When sending an initial request on behalf of a public user identity, the AS shall insert a Route header pointing to the S-CSCF where the public user identity on whose behalf the request is generated is registered or hosted (unregistered case).

NOTE 3: The address of the S-CSCF may be obtained either from a previous request terminated by the AS, by querying the HSS on the Sh interface or from static configuration.

For the use of the P-Asserted-Identity by the AS, at least two cases exist:

a) any initial request for a dialog or request for a standalone transaction is generated as if it was originated by the UE on whose behalf the request is generated. In this case the AS shall insert a P-Asserted-Identity representing a public user identity of that UE. The AS shall append the "orig" parameter to the URI of the S-CSCF; and

b) any initial request for a dialog or request for a standalone transaction is generated by an AS supporting a service identified by a PSI. In this case the AS shall insert a P-Asserted-Identity containing the PSI of the AS. Also, the AS shall append the "orig" parameter to the URI of the S-CSCF.

Editor's Note: It needs to be specified that the AS can only add the P-Asserted-Identity when the AS is within the trust domain.

The AS can indicate privacy of the P-Asserted-Identity in accordance with RFC 3323 [33], and the additional requirements contained within RFC 3325 [34].

Where privacy is required, in any initial request for a dialog or request for a standalone transaction, the AS shall set the From header to "Anonymous".

NOTE 4: The contents of the From header should not be relied upon to be modified by the network based on any privacy specified by the user either within the AS indication of privacy or by network subscription or network policy. Therefore the AS should include the value "Anonymous" whenever privacy is explicitly required.

Editor's note: Is there a need to specify any conditions for the AS choosing to indicate privacy that are generic to all originating AS, or all conditions service specific, and therefore out of the scope of 24.229.

## 5.7.4 Application Server (AS) acting as a SIP proxy

When the AS acting as a SIP proxy receives a request from the S-CSCF, prior to forwarding the request it shall:

- remove its own URI from the topmost Route header; and
- after executing the required services, route the request based on the topmost Route header.

The AS may modify the SIP requests based on service logic, prior to forwarding the request back to the S-CSCF.

The AS shall not fork the request if the fork-directive in the Request-Disposition header is set to "no-fork" as described in RFC 3841 [56B].

An AS acting as a SIP proxy shall propagate any received IM CN subsystem XML message body in the forwarded message.

When the AS acting as a SIP proxy receives an initial request for a dialog or a request for a standalone transaction, it shall store the value of the orig-ioi parameters received in the P-Charging-Vector header if present. The AS shall remove the orig-ioi parameter from the forwarded request.

NOTE: Any received orig-ioi parameters will be any type orig-ioi but includes the adjacent network term ioi in frst position. The first orig-ioi identifies the network operator from which the request was originated for a release 5 S-CSCF and the network operator from which the request was sent otherwise.

When the AS acting as a SIP proxy generates a response to an initial request for a dialog or a request for a standalone transaction, it shall insert a P-Charging-Vector header containing the orig-ioi parameters, if received in the request and a type 3 term-ioi. The AS shall set the type 3 term-ioi parameter to a value that identifies the service provider from which the response is sent and the orig-ioi parameter is set to the previously received value of orig-ioi. Any values of orig-ioi or term-ioi received in any response that is being forwarded are not used.

## 5.7.5 Application Server (AS) performing 3rd party call control

### 5.7.5.1 General

The AS performing 3rd party call control acts as a B2BUA. There are two kinds of 3rd party call control:

- Routeing B2BUA: an AS receives a request from the S-CSCF, terminates it and generates a new request, which is based on the received request.
- Initiating B2BUA: an AS initiates two requests, which are logically connected together at the AS, or an AS receives a request from the S-CSCF and initiates a new request that is logically connected but unrelated to the incoming request from the originating user (e.g. the P-Asserted-Identity of the incoming request is changed by the AS),

When the AS receives a terminated call and generates a new call, and dependent on whether the service allows the AS to change the P-Asserted-Identity for outgoing requests compared with the incoming request, the AS will select appropriate kind of 3rd party call control.

The B2BUA AS will internally map the message headers between the two dialogs that it manages. It is responsible for correlating the dialog identifiers and will decide when to simply translate a message from one dialog to the other, or when to perform other functions. These decisions are specific to each AS and are outside the scope of the present document.

The AS, although acting as a UA, does not initiate any registration of its associated addresses. These are assumed to be known by peer-to-peer arrangements within the IM CN subsystem.

For standalone transactions, when the AS is acting as a Routeing B2BUA, the AS shall copy the remaining Route header(s) unchanged from the received request for a standalone transation to the new request for a standalone transaction.

When the AS acting as a routeing B2BUA receives an initial request for a dialog or a request for a standalone transaction, it shall store the value of the orig-ioi parameters received in the P-Charging-Vector header if present. The AS shall remove the orig-ioi parameter from the forwarded request.

NOTE: Any received orig-ioi parameters will be any type orig-ioi but includes the adjacent network term ioi in frst position. The first orig-ioi identifies the network operator from which the request was originated for a release 5 S-CSCF and the network operator from which the request was sent otherwise.

When the AS acting as a routeing B2BUA generates a response to an initial request for a dialog or a request for a standalone transaction, it shall insert a P-Charging-Vector header containing the orig-ioi parameters, if received in the request and a type 3 term-ioi. The AS shall set the type 3 term-ioi parameter to a value that identifies the service provider from which the response is sent and the orig-ioi parameter is set to the previously received value of orig-ioi. Any values of orig-ioi or term-ioi received in any response that is being forwarded are not used.

### 5.7.5.2 Call initiation

#### 5.7.5.2.1 Initial INVITE

When the AS acting as a Routeing B2BUA receives an initial INVITE request from the S-CSCF, the AS shall:

- remove its own SIP URI from the topmost Route header of the received INVITE request;
- perform the AS specific functions. See 3GPP TS 23.218 [5];
- if successful, generate and send a new INVITE request to the S-CSCF to establish a new dialog;
- copy the remaining Route header(s) unchanged from the received INVITE request to the new INVITE request;
- copy the P-Asserted-Identity to the outgoing request; and
- route the new INVITE request based on the topmost Route header.

NOTE: The topmost Route header of the received INVITE request will contain the AS"s SIP URI. The following Route header will contain the SIP URI of the S-CSCF.

When the AS is acting as an Initiating B2BUA, the AS shall apply the procedures described in subclause 5.7.3 for any outgoing requests. The AS shall either set the icid parameter in the P-Charging-Vector header to be the same as received or different. The AS may retrieve CCF and/or ECF adresses from HSS on Sh interface.

#### 5.7.5.2.2 Subsequent requests

Void.

### 5.7.5.3 Call release

### 5.7.5.4 Call-related requests

An AS may initiate a call release. See 3GPP TS 23.218 [5] for possible reasons. The AS shall simultaneously send the BYE request for both dialogs managed by the B2BUA.

### 5.7.5.5 Further initial requests

When the AS acting as an Initiating B2BUA the AS shall apply the procedures described in subclause 5.7.3 for both requests. The AS shall either set the icid parameter in the P-Charging-Vector header to be the same as received or different.

## 5.7.6 Void

# 5.8 Procedures at the MRFC

## 5.8.1 General

Although the MRFC is acting as a UA, it is outside the scope of this specification how the MRFC associated addresses are made known to other entities.

When the MRFC sends any request or response (excluding ACK requests and CANCEL requests and responses) related to a dialog or standalone transaction, the MRFC may insert previously saved values into P-Charging-Vector and P-Charging-Function-Addresses headers before sending the message.

## 5.8.2 Call initiation

### 5.8.2.1 Initial INVITE

#### 5.8.2.1.1 MRFC-terminating case

##### 5.8.2.1.1.1 Introduction

The MRFC shall provide a P-Asserted-Identity header in a response to the initial request for a dialog, or any response for a standalone transaction. It is a matter of network policy whether the MRFC expresses privacy according to RFC 3323 [33] with such responses.

When the MRFC receives an initial INVITE request, the MRFC shall store the values received in the P-Charging-Vector header, e.g. icid parameter. The MRFC shall store the values received in the P-Charging-Function-Addresses header.

##### 5.8.2.1.1.2 Tones and announcements

The MRFC can receive INVITE requests to set up a session to play tones and announcements. The MRFC acts as terminating UA in this case.

When the MRFC receives an INVITE request with an indicator for a tone or announcement, the MRFC shall:

- send 100 (Trying) response.

NOTE: The detailed interfaces for requesting tones and announcements are not specified in this version of the document. Other solutions may be used in the interim.

##### 5.8.2.1.1.3 Ad-hoc conferences

The MRFC can receive INVITE requests to set up an ad-hoc conferencing session (e.g. Multiparty Call) or to add parties to the conference. The MRFC acts as terminating UA in this case.

When the MRFC receives an INVITE request with an indicator to initiate ad hoc conferencing, the MRFC shall:

- send 100 (Trying) response; and
- after the MRFP indicates that the conference resources are available, send 200 (OK) response with an MRFC conference identifier.If the MRFC chooses to send a 183 (Session Progress) response prior to the 200 (OK), then the conference identifier may also be included in the 183 (Session Progress) response.

When the MRFC receives an INVITE request with an indicator to add a party to an existing ad hoc conference (i.e. MRFC conference identifier), the MRFC shall:

- send 100 Trying response; and

- after the MRFP indicates that the conferencing request is granted, send 200 OK response with the MRFC conference identifier.If the MRFC chooses to send a 183 Session Progress response prior to the 200 OK, then the conference identifier may also be included in the 183 Session Progress response.

NOTE: The detailed interface for requesting ad-hoc conferencing sessions is not specified in this version of the document. Other solutions may be used in the interim.

#### 5.8.2.1.1.4 Transcoding

The MRFC may receive INVITE requests to set up transcoding between endpoints with incompatible codecs. The MRFC acts as terminating UA in this case.

When the MRFC receives an INVITE request with an indicator for transcoding and a codec is supplied in SDP, the MRFC shall:

- send 100 (Trying) response; and
- after the MRFP indicates that the transcoding request is granted, send 200 (OK) response.

When the MRFC receives an INVITE request with an indicator for transcoding but no SDP, the MRFC shall:

- send 183 (Session Progress) response with list of codecs supported by the MRFC/MRFP.

### 5.8.2.1.2 MRFC-originating case

The MRFC shall provide a P-Asserted-Identity header in an initial request for a dialog, or any request for a standalone transaction. It is a matter of network policy whether the MRFC expresses privacy according to RFC 3323 [33] with such requests.

When an MRFC generates an initial request for a dialog or a request for a standalone transaction, the MRFC shall insert a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.260 [17].

## 5.8.2.2 Subsequent requests

### 5.8.2.2.1 Tones and announcements

When the MRFC receives an ACK request for a session, this may be considered as an event to direct the MRFP to start the playing of a tone or announcement.

# 5.8.3 Call release

## 5.8.3.1 S-CSCF-initiated call release

### 5.8.3.1.1 Tones and announcements

When the MRFC receives a BYE request for a session, the MRFC directs the MRFP to stop the playing of a tone or announcement.

## 5.8.3.2 MRFC-initiated call release

### 5.8.3.2.1 Tones and announcements

When the MRFC has a timed session to play tones and announcements and the time expires, the MRFC shall:

- send a BYE request towards the UE.

When the MRFC is informed by the MRFP that tone or announcement resource has been released, the MRFC shall:

- send a BYE request towards the UE.

#### 5.8.2.2.2 Transcoding

When the MRFC receives a PRACK request (in response to the 183 (Session Progress) response) with an indicator for transcoding and codec supplied in SDP, the MRFC shall:

- after the MRFP indicates that the transcoding request is granted, send 200 (OK) response.

## 5.8.4 Call-related requests

### 5.8.4.1 ReINVITE

#### 5.8.4.1.1 MRFC-terminating case

##### 5.8.4.1.1.1 Ad-hoc conferences

The MRFC can receive reINVITE requests to modify an ad-hoc conferencing session (e.g. Multiparty Call) for purposes of floor control and for parties to leave and rejoin the conference.

When the MRFC receives a reINVITE request, the MRFC shall:

- send 100 (Trying) response; and
- after the MRFP indicates that the conferencing request is granted, send 200 (OK) response with the MRFC conference identifier.If the MRFC chooses to send a 183 (Session Progress) response prior to the 200 OK, then the conference identifier may also be included in the 183 (Session Progress) response.

NOTE: The detailed interface for requesting ad-hoc conferencing sessions is not specified in this version of the document. Other solutions may be used in the interim.

#### 5.8.4.1.2 MRFC-originating case

Void.

### 5.8.4.2 REFER

#### 5.8.4.2.1 MRFC-terminating case

Void.

#### 5.8.4.2.2 MRFC-originating case

Void.

#### 5.8.4.2.3 REFER initiating a new session

Void.

#### 5.8.4.2.4 REFER replacing an existing session

Void.

### 5.8.4.3 INFO

Void.

### 5.8.5 Further initial requests

When the MRFC responds to an OPTIONS request with a 200 (OK) response, the MRFC may include a message body with an indication of the supported tones/announcement packages, DTMF capabilities, supported codecs and conferencing options of the MRFC/MRFP.

NOTE: The detailed interface for requesting MRFC/MRFP capabilities is not specified in this version of the document. Other solutions may be used in the interim.

## 5.9 IMS-ALG

### 5.9.1 General

The IMS-ALG acts as a B2BUA. The IMS-ALG will internally map the message headers between the two dialogs that it manages. It is responsible for correlating the dialog identifiers and will decide when to simply translate a message from one dialog to the other, or when to perform other functions. The IMS-ALG, although acting as a UA, does not initiate any registration of its associated addresses. These are assumed to be known by peer-to-peer arrangements within the IM CN subsystem. The use of the Path and Service-Route headers shall not be supported by the IMS-ALG.

When the IMS-ALG receives an initial INVITE request from a SIP network that does not support the IP address type used in the IM CN subsystem, the IMS-ALG shall generate a new initial INVITE request and forward it to the I-CSCF.

The internal function of the IMS-ALG is defined in 3GPP TS 29.162 [11A].

# 6 Application usage of SDP

## 6.1 Procedures at the UE

### 6.1.1 General

The "integration of resource management and SIP" extension is hereafter in this subclause referred to as "the precondition mechanism" and is defined in RFC 3312 [30] as updated by RFC 4032 [64].

In order to authorize the media streams, the P-CSCF and S-CSCF have to be able to inspect the SDP payloads. Hence, the UE shall not encrypt the SDP payloads.

During session establishment procedure, SIP messages shall only contain SDP payload if that is intended to modify the session description, or when the SDP payload must be included in the message because of SIP rules described in RFC 3261[26].

For "video" and "audio" media types that utilize the RTP/RTCP, the UE shall specify the proposed bandwidth for each media stream utilizing the "b=" media descriptor and the "AS" bandwidth modifier in the SDP.

If the media line in the SDP indicates the usage of RTP/RTCP, in addition to the "AS" bandwidth modifier in the media-level "b=" line, the UE shall include two media-level "b=" lines, one with the "RS" bandwidth modifier and the other with the "RR" bandwidth modifier as described in RFC 3556 [56] to specify the required bandwidth allocation for RTCP.

For other media streams the "b=" media descriptor may be included. The value or absence of the "b=" parameter will affect the assigned QoS which is defined in 3GPP TS 29.208 [13].

NOTE 1: In a two-party session where both participants are active, the RTCP receiver reports are not sent, therefore, the RR bandwidth modifer will typically get the value of zero.

The UE shall include the MIME subtype "telephone-event" in the "m=" media descriptor in the SDP for audio media flows that support both audio codec and DTMF payloads in RTP packets as described in RFC 2833 [23].

The UE shall inspect the SDP contained in any SIP request or response, looking for possible indications of grouping of media streams according to RFC 3524 [54] and perform the appropriate actions for IP-CAN bearer establishment for media according to IP-CAN specific procedures (see subclause B.2.2.5 for IP-CAN implemented using GPRS).

If resource reservation is needed, the UE shall start reserving its local resources whenever it has sufficient information about the media streams, media authorization and used codecs available.

NOTE 2: Based on this resource reservation can, in certain cases, be initiated immediately after the sending or receiving of the initial SDP offer.

In order to fulfil the QoS requirements of one or more media streams, the UE may re-use previously reserved resources. In this case the local preconditions related to the media stream, for which resources are re-used, shall be indicated as met.

If an IP-CAN bearer is rejected or modified, the UE shall, if the SDP is affected, update the remote SIP entity according to RFC 3261 [26] and RFC 3311 [29].

## 6.1.2 Handling of SDP at the originating UE

An INVITE request generated by a UE shall contain a SDP offer. The SDP offer shall reflect the calling user's terminal capabilities and user preferences for the session. The UE shall order the SDP offer with the most preferred codec listed first.

If the desired QoS resources for one or more media streams have not been reserved at the UE when constructing the initial SDP offer, the UE shall:

- indicate the related local preconditions for QoS as not met, using the segmented status type, as defined in RFC 3312 [30] and RFC 4032[64], as well as the strength-tag value "mandatory" for the local segment and the strength-tag value "optional" for the remote segment, if the UE supports the precondition mechanism (see subclause 5.1.3.1); and,

- set the related media streams to inactive, by including an "a=inactive" line, according to the procedures described in draft-ietf-mmusic-sdp-new [39].

NOTE 1: When setting the media streams to the inactive mode, the UE can include in the first SDP offer the proper values for the RS and RR modifiers and associate bandwidths to prevent the receiving of the RTCP packets, and not send any RTCP packets.

If the desired QoS resources for one or more media streams are available at the UE when the initial SDP offer is sent, the UE shall indicate the related local preconditions as met, using the segmented status type, as defined in RFC 3312 [30] and RFC 4032[64], as well as the strength-tag value "mandatory" for the local segment and the strength-tag value "optional" for the remote segment, if the UE supports the precondition mechanism (see subclause 5.1.3.1).

NOTE 2: If the originating UE does not support the precondition mechanism it will not include any precondition information in SDP.

Upon generating the SDP offer for an INVITE request generated after receiving a 488 (Not Acceptable Here) response, as described in subclause 5.1.3.1, the UE shall include SDP payload containing a subset of the allowed media types, codecs and other parameters from the SDP payload of all 488 (Not Acceptable Here) responses related to the same session establishment attempt (i.e. a set of INVITE requests used for the same session establishment). The UE shall order the codecs in the SDP payload according to the order of the codecs in the SDP payload of the 488 (Not Acceptable Here) response.

NOTE 3: The UE can attempt a session establishment through multiple networks with different policies and potentially can need to send multiple INVITE requests and receive multiple 488 (Not Acceptable Here) responses from different CSCF nodes. The UE therefore takes into account the SDP contents of all the 488 (Not Acceptable Here) responses received related to the same session establishment when building a new INVITE request.

Upon confirming successful local resource reservation, the UE shall create a SDP offer in which the media streams previously set to inactive mode are set to active (sendrecv, sendonly or recvonly) mode.

### 6.1.3 Handling of SDP at the terminating UE

Upon receipt of an initial SDP offer in which no precondition information is available, the UE shall in the SDP answer:

- if the desired QoS resources for one or more media streams have not been reserved at the terminating UE, set the related media streams to inactive mode by including an "a=inactive" line, according to the procedures described in draft-ietf-mmusic-sdp-new [39]; or

- if, prior to sending the SDP answer the desired QoS resources have been reserved at the terminating UE, set the related media streams to active mode in the SDP answer.

If the terminating UE had previously set one or more media streams to inactive mode and the QoS resources for those media streams are now ready, it shall set the media streams to active mode by applying the procedures described in draft-ietf-mmusic-sdp-new [39] with respect to setting the direction of media streams.

Upon sending a SDP answer to an initial SDP offer (which included one or more media lines which was offered with several codecs) the terminating UE shall select exactly one codec per payload and indicate only the selected codec for the related media stream.

NOTE 1: A SDP media line can indicate several different payloads. For example a media line indicating an audio media type can indicate several codecs for the audio stream as well as the MIME subtype "telephone-event" for DTMF payload.

Upon sending a SDP answer to an initial SDP offer, with the SDP answer including one or more media streams for which the originating side did indicate its local preconditions as not met, if the precondition mechanism is supported by the terminating UE, the terminating UE shall indicates its local preconditions and request the confirmation for the result of the resource reservation at the originating end point.

NOTE 2: If the terminating UE does not support the precondition mechanism it will ignore any precondition information received from the originating UE.

Upon receipt an initial INVITE request, that includes the SDP offer containing an IP address type (in the "c=" parameter) that is not supported by the UE, it shall respond with the 488 (Not Acceptable Here) response with 301 Warning header indicating "incompatible network address format".

## 6.2 Procedures at the P-CSCF

When the P-CSCF receives any SIP request containing an SDP offer, the P-CSCF shall examine the media parameters in the received SDP. If the P-CSCF finds any media parameters which are not allowed on the network by local policy, the P-CSCF shall return a 488 (Not Acceptable Here) response containing SDP payload. This SDP payload contains either all the media types, codecs and other SDP parameters which are allowed according to the local policy, or, based on configuration by the operator of the P-CSCF, a subset of these allowed parameters. This subset may depend on the content of the received SIP request. The P-CSCF shall build the SDP payload in the 488 (Not Acceptable Here) response in the same manner as a UAS builds the SDP in a 488 (Not Acceptable Here) response as specifed in RFC 3261 [26]. The P-CSCF shall order the SDP payload with the most preferred codec listed first. If the SDP offer is encrypted, the P-CSCF may reject the request.

When the P-CSCF receives a SIP response different from 200 (OK) response containing SDP offer, the P-CSCF shall not examine the media parameters in the received SDP offer, but the P-CSCF shall rather check the succeeding request containing the SDP answer for this offer, and if necessary (i.e. the SDP answer reduced by the UE still breaches local policy), the P-CSCF shall return a 488 (Not Acceptable Here) response containing the local policy allowed SDP payload. If the SDP answer is encrypted, the P-CSCF may reject the succeeding request.

When the P-CSCF receives a 200 (OK) response containing SDP offer, the P-CSCF shall examine the media parameters in the received SDP. If the P-CSCF finds any media parameters which are not allowed on the network by local policy, the P-CSCF shall forward the SDP offer and on the receipt of the ACK request containing the SDP answer, it shall immediately terminate the session as described in subclause 5.2.8.1.2. If the SDP offer is encrypted, the P-CSCF shall forward the SDP offer and on the receipt of the ACK request containing the SDP answer, it may immediately terminate the session as described in subclause 5.2.8.1.2.

When the P-CSCF receives an initial INVITE request for a terminating session setup or a 183 (Session Progress) response to an INVITE request for an originating session setup, the P-CSCF may modify the SDP according to RFC 3524 [54] to indicate to the UE that particular media stream(s) is grouped according to a local policy. The policy is

used to determine whether the P-CSCF will request the UE to keep media stream(s) grouped in different IP-CAN bearers and identify the relation between different media streams and IP-CAN bearers (see subclause B.2.2.5 for IP-CAN implemented using GPRS).

The P-CSCF shall apply and maintain the same policy within the SDP from the initial request or response containing SDP and throughout the complete SIP session. If a media stream is added and grouping of media streams apply to the session, the P-CSCF shall modify the SDP according to RFC 3524 [54] to indicate to the UE that the added media stream(s) will be grouped into either a new group or into one of the existing groups. The P-CSCF shall not indicate re-grouping of media stream(s) within the SDP.

The P-CSCF shall not apply RFC 3524 [54] to the SDP for additional media stream(s), if grouping of media stream(s) was not indicated in the initial INVITE request or 183 (Session Progress) response.

The P-CSCF may inspect, if present, the "b=RS" and "b=RR" lines in order to find out the bandwidth allocation requirements for RTCP.

# 6.3 Procedures at the S-CSCF

When the S-CSCF receives any SIP request containing an SDP offer, the S-CSCF shall examine the media parameters in the received SDP. If the S-CSCF finds any media parameters which are not allowed based on either local policy or the subscription, the S-CSCF shall return a 488 (Not Acceptable Here) response containing SDP payload. This SDP payload contains either all the media types, codecs and other SDP parameters which are allowed according to the local policy and users subscription or, based on configuration by the operator of the S-CSCF, a subset of these allowed parameters. This subset may depend on the content of the received SIP request. The S-CSCF shall build the SDP payload in the 488 (Not Acceptable Here) response in the same manner as a UAS builds the SDP in a 488 (Not Acceptable Here) response as specified in RFC 3261 [26]. If the SDP offer is encrypted, the S-CSCF may reject the request.

When the S-CSCF receives a SIP response different from 200 (OK) response containing SDP offer, the S-CSCF shall not examine the media parameters in the received SDP offer, but the S-CSCFshall rather check the succeeding request containing the SDP answer for this offer, and if necessary (i.e. the SDP answer reduced by the UE still breaches local policy), the S-CSCF shall return a 488 (Not Acceptable Here) response containing the local policy allowed SDP payload. If the SDP answer is encrypted, the S-CSCF may reject the succeeding request.

When the S-CSCF receives a 200 (OK) response containing SDP offer, the S-CSCF shall examine the media parameters in the received SDP. If the S-CSCF finds any media parameters which are not allowed based on either local policy or the subscription, the S-CSCF shall forward the SDP offer and on the receipt of the ACK request containing the SDP answer, it shall immediately terminate the session as described in subclause 5.4.5.1.2. If the SDP offer is encrypted, the S-CSCF shall forward the SDP offer and on the receipt of the ACK request containing the SDP answer, it may immediately terminate the session as described in subclause 5.4.5.1.2.

# 6.4 Procedures at the MGCF

## 6.4.1 Calls originating from circuit-switched networks

The usage of SDP by the MGCF is the same as its usage by the UE, as defined in the subclause 6.1 and A.3.2, with the following exception:

- In an INVITE request generated by a MGCF, the MGCF shall indicate the current status of the precondition.

When sending an SDP, the MGCF shall not include the "i=", "u=", "e=", "p=", "r=", and "z=" descriptors in the SDP, and it shall ignore them when received in the SDP.

When the MGCF generates and sends an INVITE request for a call originating in a circuit-switched network, the MGCF shall:

- populate the SDP with the codecs supported by the associated MGW (see 3GPP TS 26.235 [10] for the supported codecs); and

- in order to support DTMF, populate the SDP with MIME subtype "telephone-event" as described in RFC 2833 [23].

When the MGCF receives 183 (Session Progress) response to an INVITE request, the MGCF shall:

- check that a supported codec has been indicated in the SDP.

### 6.4.2 Calls terminating in circuit-switched networks

The usage of SDP by the MGCF is the same as its usage by the UE, as defined in the subclause 6.1 and A.3.2, with the following exception:

- When the MGCF sends a 183 (Session Progress) response with SDP payload, it shall only request confirmation for the result of the resource reservation at the originating end point if there are any remaining unfulfilled preconditions.

When sending an SDP, the MGCF shall not include the "i=", "u=", "e=", "p=", "r=", and "z=" descriptors in the SDP, and it shall ignore them when received in the SDP.

When the MGCF receives an initial INVITE request, the MGCF shall:

- check for a codec that matches the requested SDP, which may include the MIME subtype "telephone-event" as described in RFC 2833 [23].

When the MGCF generates and sends a 183 (Session Progress) response to an initial INVITE request, the MGCF shall:

- set SDP indicating the selected codec, which may include the MIME subtype "telephone-event" as described in RFC 2833 [23].

## 6.5 Procedures at the MRFC

Void.

## 6.6 Procedures at the AS

Since an AS may provide a wide range of different services, procedures for the SDP usage for an AS acting as originating UA, terminating UA or third-party call control role are dependent on the service provided to the UA and on the capabilities on the remote UA. There is no special requirements regarding the usage of the SDP, except the requirements for the SDP capabilities described in the following paragraphs and clause A.3:

1) Providing that an INVITE request generated by an AS contains SDP payload, the AS has the capability of reflecting the originating AS's capabilities, desired QoS and precondition requirements for the session in the SDP payload.

2) When the AS sends a 183 (Session Progress) response with SDP payload including one or more "m=" media types, it has the capability of requesting confirmation for the result of the resource reservation at the originating endpoint.

## 6.7 Procedures at the IMS-ALG

IMS-ALG makes procedures as for an originating UA and terminating UA. The IMS-ALG acts as a B2BUA. The treatment of the SDP information between originating UA and terminating UA is described in 3GPP TS 29.162 [11A].

# 7 Extensions within the present document

## 7.1 SIP methods defined within the present document

There are no SIP methods defined within the present document over and above those defined in the referenced IETF specifications.

## 7.2 SIP headers defined within the present document

### 7.2.0 General

There are no SIP headers defined within the present document over and above those defined in the referenced IETF specifications.

### 7.2.1 Void

### 7.2.2 Void

### 7.2.3 Void

### 7.2.4 Void

### 7.2.5 Void

### 7.2.6 Void

### 7.2.7 Void

### 7.2.8 Void

### 7.2.9 Void

### 7.2.10 Void

## 7.2A Extensions to SIP headers defined within the present document

### 7.2A.1 Extension to WWW-authenticate header

#### 7.2A.1.1 Introduction

This extension defines a new authentication parameter (auth-param) for the WWW-Authenticate header used in a 401 (Unauthorized) response to the REGISTER request. For more information, see RFC 2617 [21] subclause 3.2.1.

#### 7.2A.1.2 Syntax

The syntax for for auth-param is specified in table 7.4.

**Table 7.4: Syntax of auth-param**

```
auth-param      = 1#( integrity-key / cipher-key )
integrity-key   = "ik" EQUAL ik-value
cipher-key      = "ck" EQUAL ck-value
ik-value        = LDQUOT *(HEXDIG) RDQUOT
ck-value        = LDQUOT *(HEXDIG) RDQUOT
```

#### 7.2A.1.3 Operation

This authentication parameter will be used in a 401 (Unauthorized) response in the WWW-authenticate header during UE authentication procedure as specified in subclause 5.4.1.

The S-CSCF appends the integrity-key parameter (directive) to the WWW.-Authenticate header in a 401 (Unauthorized) response. The P-CSCF stores the integrity-key value and removes the integrity-key parameter from the header prior to forwarding the response to the UE.

The S-CSCF appends the cipher-key parameter (directive) to the WWW-Authenticate header in a 401 (Unauthorized) response. The P-CSCF removes the cipher-key parameter from the header prior to forwarding the response to the UE. In the case ciphering is used, the P-CSCF stores the cipher-key value.

### 7.2A.2 Extension to Authorization header

#### 7.2A.2.1 Introduction

This extension defines a new auth-param for the Authorization header used in REGISTER requests. For more information, see RFC 2617 [21] subclause 3.2.2.

#### 7.2A.2.2 Syntax

The syntax of auth-param for the Authorization header is specified in table 7.5.

**Table 7.5: Syntax of auth-param for Authorization header**

```
auth-param = 'integrity-protected' EQUAL ('yes' / 'no')
```

#### 7.2A.2.3 Operation

This authentication parameter is inserted by the P-CSCF in the Authorization header of all the REGISTER requests received from the UE. The value of the "integrity protected" field in the auth-param parameter is set as specified in subclause 5.2.2. This information is used by S-CSCF to decide whether to challenge the REGISTER request or not, as specified in subclause 5.4.1.

### 7.2A.3 Tokenized-by parameter definition (various headers)

#### 7.2A.3.1 Introduction

The tokenized-by parameter is an extension parameter appended to encrypted entries in various SIP headers as defined in subclause 5.3.3.1.

#### 7.2A.3.2 Syntax

The syntax for the tokenized-by parameter is specified in table 7.6:

**Table 7.6: Syntax of tokenized-by-param**

```
uri-parameter =  transport-param / user-param / method-param
/ ttl-param / maddr-param / lr-param / tokenized-by-param / other-param
tokenized-by-param = 'tokenized-by' EQUAL hostname
```

The BNF for uri-parameter is taken from IETF RFC 3261 [26] and modified accordingly.

### 7.2A.3.3 Operation

The tokenized-by parameter is appended by I-CSCF(THIG) after all encrypted strings within SIP headers when network configuration hiding is active. The value of the parameter is the domain name of the network which encrypts the information.

## 7.2A.4 P-Access-Network-Info header

### 7.2A.4.1 Introduction

The P-Access-Network-Info header is extended to include specific information relating to particular access technologies.

### 7.2A.4.2 Syntax

The syntax of the P-Access-Network-Info header is described in RFC 3455 [52]. There are additional coding rules for this header depending on the type of IP-CAN, according to access technology specific descriptions.

Table 7.6A describes 3GPP-specific extensions to the P-Charging-Vector header field defined in RFC 3455 [52].

**Table 7.6A: Syntax of extensions to P-Access-Network-Info header**

```
   access-type           = "IEEE-802.11" / "IEEE-802.11a" / "IEEE-802.11b" / "IEEE-802.11g" /
                           "3GPP-GERAN" / "3GPP-UTRAN-FDD" / "3GPP-UTRAN-TDD" / "3GPP2-1X" /
                           "3GPP2-1X-HRPD" /token
   access-info           = cgi-3gpp / utran-cell-id-3gpp / ci-3gpp2/ extension- access-info
   extension-access-info = gen-value
   cgi-3gpp              = "cgi-3gpp" EQUAL (token / quoted-string)
   utran-cell-id-3gpp    = "utran-cell-id-3gpp" EQUAL (token / quoted-string)
   ci-3gpp2              = "ci-3gpp2" EQUAL (token / quoted-string)
```

### 7.2A.4.3 Additional coding rules for P-Access-Network-Info header

The UE shall populate the P-Access-Network-Info header, where use is specified in subclause 5.1, with the following contents:

1) the access-type field set to one of "3GPP-GERAN","3GPP-UTRAN-FDD", "3GPP-UTRAN-TDD", "3GPP2-1X", "3GPP2-1X-HRPD", "IEEE-802.11" or "IEEE-802.11a" or "IEEE-802.11b" or "IEEE-802.11g" as appropriate to the radio access technology in use;

2) if the access type field is set to "3GPP-GERAN", a cgi-3gpp parameter set to the Cell Global Identity obtained from lower layers of the UE. The Cell Global Identity is a concatenation of MCC, MNC, LAC and CI (as described in 3GPP TS 23.003 [3]). The value of "cgi-3gpp" parameter is therefore coded as a text string as follows:

   Starting with the most significant bit, MCC (3 digits), MNC (2 or 3 digits depending on MCC value), LAC (fixed length code of 16 bits using full hexadecimal representation) and CI (fixed length code of 16 bits using a full hexadecimal representation);

3) if the access type field is equal to "3GPP-UTRAN-FDD", or "3GPP-UTRAN-TDD", a "utran-cell-id-3gpp" parameter set to a concatenation of the MCC, MNC, LAC (as described in 3GPP TS 23.003 [3]) and the UMTS

Cell Identity (as described in 3GPP TS 25.331 [9A]), obtained from lower layers of the UE, and is coded as a text string as follows:

Starting with the most significant bit, MCC (3 digits), MNC (2 or 3 digits depending on MCC value), LAC (fixed length code of 16 bits using full hexadecimal representation) and UMTS Cell Identity (fixed length code of 28 bits);

4) if the access type field is set to "3GPP2-1X", a ci-3gpp2 parameter set to the ASCII representation of the hexadecimal value of the string obtained by the concatenation of SID (16 bits), NID (16 bits), PZID (8 bits) and BASE_ID (16 bits) (see 3GPP2 C.S0005-D [85]) in the specified order. The length of the ci-3gpp2 parameter shall be 14 hexadecimal characters. The hexadecimal characters (A through F) shall be coded using the uppercase ASCII characters. If the MS does not know the values for any of the above parameters, the MS shall use the value of 0 for that parameter. For example, if the SID is unknown, the MS shall represent the SID as 0x0000;

NOTE 1: The SID value is represented using 16 bits as supposed to 15 bits as specified in 3GPP2 C.S0005-D [85].

EXAMPLE: If SID = 0x1234, NID = 0x5678, PZID = 0x12, BASE_ID = 0xFFFF, the ci-3gpp2 value is set to the string "1234567812FFFF".

5) if the access type field is set to "3GPP2-1X-HRPD", a ci-3gpp2 parameter set to the ASCII representation of the hexadecimal value of the string obtained by the concatenation of Sector ID (128 bits) and Subnet length (8 bits) (see 3GPP2 C.S0024-A [86]) in the specified order. The length of the ci-3gpp2 parameter shall be 34 hexadecimal characters. The hexadecimal characters (A through F) shall be coded using the uppercase ASCII characters;

EXAMPLE: If the Sector ID = 0x12341234123412341234123412341234, Subnet length = 0x11, the ci-3gpp2 value is set to the string "12341234123412341234123412341234123411".

6) if the access-type field set to one of "IEEE-802.11" or "IEEE-802.11a" or "IEEE-WLAN-802.11b" or "IEEE-802.11g" the access info parameter is set to a null value. This release of this specification does not define values for use in this parameter.

## 7.2A.5 P-Charging-Vector header

### 7.2A.5.1 Introduction

The P-Charging-Vector header field is extended to include specific charging correlation information needed for IM CN subsystem functional entities.

### 7.2A.5.2 Syntax

#### 7.2A.5.2.1 General

The syntax of the P-Charging-Vector header field is described in RFC 3455 [52]. There may be additional coding rules for this header depending on the type of IP-CAN, according to access technology specific descriptions.

Table 7.3 describes 3GPP-specific extensions to the P-Charging-Vector header field defined in RFC 3455 [52].

**Table 7.3: Syntax of extensions to P-Charging-Vector header**

```
access-network-charging-info = (gprs-charging-info / i-wlan-charging-info / generic-param)
gprs-charging-info = ggsn SEMI auth-token [SEMI pdp-info-hierarchy] *(SEMI extension-param)
ggsn = "ggsn" EQUAL gen-value
pdp-info-hierarchy = "pdp-info" EQUAL LDQUOT pdp-info *(COMMA pdp-info) RDQUOT
pdp-info = pdp-item SEMI pdp-sig SEMI gcid [SEMI flow-id]
pdp-item = "pdp-item" EQUAL DIGIT
pdp-sig = "pdp-sig" EQUAL ("yes" / "no")
gcid = "gcid" EQUAL 1*HEXDIG
auth-token = "auth-token" EQUAL 1*HEXDIG
flow-id = "flow-id" EQUAL "(" "{" 1*DIGIT COMMA 1*DIGIT "}" *(COMMA "{" 1*DIGIT COMMA 1*DIGIT
     "}")")"
extension-param = token [EQUAL token]
i-wlan-charging-info = "pdg"
```

The access-network-charging-info parameter is an instance of generic-param from the current charge-params component of P-Charging-Vector header.

The access-network-charging-info parameter includes alternative definitions for different types access networks. The description of these parameters are given in the subsequent subclauses.

The access network charging information is not included in the P-Charging-Vector for SIP signalling that is not associated with a session,

When the access network charging information is included in the P-Charging-Vector and necessary information is not available from the Go/Gq interface reference points then null or zero values are included

For type 1 and type 3 IOIs, the generating SIP entity shall express the orig-ioi and term-ioi parameters in the format of a quoted string as specified in RFC 3455 [52] with a specific string prefix being "Type 1" and "Type 3" respectively to indicate the type of IOI. For the type 2 IOI, no string prefix is used. The receiving SIP entity does not perform syntactic checking of the contents of the IOI parameter (the IOI parameter is passed unmodified to charging entities).

#### 7.2A.5.2.2 GPRS as IP-CAN

GPRS is the initially supported access network (gprs-charging-info parameter). For GPRS there are the following components to track: GGSN address (ggsn parameter), media authorization token (auth token parameter), and a pdp-info parameter that contains the information for one or more PDP contexts. The pdp-info contains one or more pdp-item values followed by a collection of parameters (pdp-sig, gcid, and flow-id). The value of the pdp-item is a unique number that identifies each of the PDP-related charging information within the P-Charging-Vector header. Each PDP context has an indicator if it is an IM CN subsystem signalling PDP context (pdp-sig parameter), an associated GPRS Charging Identifier (gcid parameter), and a identifier (flow-id parameter). The flow-id parameter contains a sequence of curly bracket delimited flow identifier tuples that identify associated m-lines and relative order of port numbers in an m-line within the SDP from the SIP signalling to which the PDP context charging information applies. For a complete description of the semantics of the flow-id parameter see 3GPP TS 29.207 [12] Annex C. The gcid, ggsn address and flow-id parameters are transferred from the GGSN to the P-CSCF via the PDF over the Go interface (see 3GPP TS 29.207 [12]) and Gq interface (see 3GPP TS 29.209 [13A]).

The gcid value is received in binary format at the P-CSCF (see 3GPP TS 29.207 [12]). The P-CSCF shall encode it in hexadecimal format before include it into the gcid parameter. On receipt of this header, a node receiving a gcid shall decode from hexadecimal into binary format.

The access network charging information is not included in the P-Charging-Vector for SIP signalling may not be available for sessions that use a general purpose PDP context (for both SIP signalling and media) or that do not require media authorisation.

#### 7.2A.5.2.3 I-WLAN as IP-CAN

The access-network-charging-info parameter is an instance of generic-param from the current charge-params component of P-Charging-Vector header.

This version of the specification defines the use of "pdg" for inclusion in the P-Charging-Vector header. No other extensions are defined for use in I-WLAN in this version of the specification.

### 7.2A.5.3 Operation

The operation of this header is described in subclauses 5.2, 5.3, 5.4, 5.5, 5.6, 5.7 and 5.8.

## 7.2A.6 Orig parameter definition

Editor"s note: According to draft-ietf-sip-uri-parameter-reg-01, all SIP and SIPS URI parameters MUST be documented in an RFC in order to be registered by IANA. Registered SIP or SIPS URI parameters are to be considered "reserved words". 3GPP shall consider to describe this parameter in an informational RFC and register it by IANA. When that happens, section 7.2A.6 will be removed.

### 7.2A.6.1 Introduction

The "orig" parameter is a uri-parameter intended to tell to the S-CSCF that it has to perform the originating services instead of terminating services.

### 7.2A.6.2 Syntax

The syntax for the orig parameter is specified in table 7.7:

**Table 7.7: Syntax of orig parameter**

```
uri-parameter =  transport-param / user-param / method-param / ttl-param / maddr-param / lr-param /
    orig / other-param
orig = 'orig'
```

The BNF for uri-parameter is taken from IETF RFC 3261 [26] and modified accordingly.

### 7.2A.6.3 Operation

The orig parameter is appended to the address of the S-CSCF by the ASs, when those initiate requests on behalf of the user. The S-CSCF will run originating services whenever the orig parameter is present next to its address.

## 7.2A.7 Extension to Security-Client, Security-Server and Security-Verify headers

### 7.2A.7.1 Introduction

This extension defines new paramerts for the Security-Client, Security-Server and Security-Verify headers.

### 7.2A.7.2 Syntax

The syntax for the Security-Client, Security-Server and Security-Verify headers is defined in IETF RFC 3329. The additional syntax is defined in Annex H of 3GPP TS 33.203 [19].

### 7.2A.7.3 Operation

The operation of the additional parameters for the Security-Client, Security-Server and Security-Verify headers is defined in Annex H of 3GPP TS 33.203 [19].

# 7.3 Option-tags defined within the present document

There are no option-tags defined within the present document over and above those defined in the referenced IETF specifications.

## 7.4 Status-codes defined within the present document

There are no status-codes defined within the present document over and above those defined in the referenced IETF specifications.

## 7.5 Session description types defined within the present document

There are no session description types defined within the present document over and above those defined in the referenced IETF specifications.

## 7.6 3GPP IM CN subsystem XML body, version 1

### 7.6.1 General

This subclause describes the Document Type Definition that is applicable for the 3GPP IM CN Subsystem XML body.

Any SIP User Agent or proxy may insert or remove the 3GPP IM CN subsystem XML body or parts of it, as required, in any SIP message. The 3GPP IM CN subsystem XML body shall not be forwarded outside a 3GPP network.

The associated MIME type with the 3GPP IMS XML body is "application/3gpp-ims+xml".

### 7.6.2 Document Type Definition

The Document Type Definition, according to XML syntax definitions, is defined in table 7.7.

**Table 7.7: IM CN subsystem XML body, version 1 DTD**

```
<?xml version="1.0" ?>
<!-- Draft DTD for the IMS XML body. -->

<!DOCTYPE ims-3gpp [
    <!-- ims-3gpp element: root element -->

    <!ELEMENT ims-3gpp (
        alternative-service?, service-info?)>
    <!ATTLIST ims-3gpp version CDATA #REQUIRED>

    <!-- service-info element: The transparent data received from HSS for AS -->
    <!ELEMENT service-info              (#CDATA)>

    <!-- alternative-service: alternative-service used in emergency sessions -->
    <!ELEMENT alternative-service   (type, reason)>
    <!ELEMENT type                  (emergency)>
    <!ELEMENT reason                (#PCDATA)>

]>
```

### 7.6.3 DTD description

This subclause describes the elements of the IMS Document Type Definition as defined in table 7.7.

<ims-3gpp>: This is the root element of the IMS XML body. It shall always be present. The version described in the present document is 1.

<service-info>: the transparent element received from the HSS for a particular trigger point are placed within this optional element.

<alternative-service>: in the present document, the alternative service is used as a response for an attempt to establish an emergency session within the IM CN subsystem. The element describes an alternative service where the call should success. The alternative service is described by the type of service information. A possible reason cause why an alternative service is suggested may be included.

The <alternative-service> element contains a <type> element that indicates the type of alternative service. In the present document, the <type> element contains only the value "emergency".

The <reason> element contains an explanatory text with the reason why the session setup has been redirected. A UE may use this information to give an indication to the user.

## 7.7 SIP timers

The timers defined in RFC 3261 [26] need modification in some cases to accommodate the delays introduced by the air interface processing and transmission delays. Table 7.8 shows recommended values for IM CN subsystem.

Table 7.8 lists in the first column, titled "SIP Timer" the timer names as defined in RFC 3261 [26].

The second column, titled "value to be applied between IM CN subsystem elements" lists the values recommended for network elements e.g. P-CSCF, S-CSCF, MGCF, when communicating with each other i.e. when no air interface leg is included. These values are identical to those recommended by RFC 3261 [26].

The third column, titled "value to be applied at the UE" lists the values recommended for the UE. These are modified when compared to RFC 3261 [26] to accommodate the air interface delays.

The fourth column, titled "value to be applied at the P-CSCF toward a UE" lists the values recommended for the P-CSCF when an air interface leg is traversed. These are modified when compared to RFC 3261 [26].

The final column reflects the timer meaning as defined in RFC 3261 [26].

**Table 7.8: SIP timers**

| SIP Timer | Value to be applied between IM CN subsystem elements | Value to be applied at the UE | Value to be applied at the P-CSCF toward a UE | Meaning |
|---|---|---|---|---|
| T1 | 500ms default | 2s default | 2s default | RTT estimate |
| T2 | 4s | 16s | 16s | The maximum retransmit interval for non-INVITE requests and INVITE responses |
| T4 | 5s | 17s | 17s | Maximum duration a message will remain in the network |
| Timer A | initially T1 | initially T1 | initially T1 | INVITE request retransmit interval, for UDP only |
| Timer B | 64*T1 | 64*T1 | 64*T1 | INVITE transaction timeout timer |
| Timer C | > 3min | > 3 min | > 3 min | proxy INVITE transaction timeout |
| Timer D | > 32s for UDP | >128s | >128s | Wait time for response retransmits |
| | 0s for TCP/SCTP | 0s for TCP/SCTP | 0s for TCP/SCTP | |
| Timer E | initially T1 | initially T1 | initially T1 | non-INVITE request retransmit interval, UDP only |
| Timer F | 64*T1 | 64*T1 | 64*T1 | non-INVITE transaction timeout timer |
| Timer G | initially T1 | initially T1 | initially T1 | INVITE response retransmit interval |
| Timer H | 64*T1 | 64*T1 | 64*T1 | Wait time for ACK receipt. |
| Timer I | T4 for UDP | T4 for UDP | T4 for UDP | Wait time for ACK retransmits |
| | 0s for TCP/SCTP | 0s for TCP/SCTP | 0s for TCP/SCTP | |
| Timer J | 64*T1 for UDP | 64*T1 for UDP | 64*T1 for UDP | Wait time for non-INVITE request retransmits |
| | 0s for TCP/SCTP | 0s for TCP/SCTP | 0s for TCP/SCTP | |
| Timer K | T4 for UDP | T4 for UDP | T4 for UDP | Wait time for response retransmits |
| | 0s for TCP/SCTP | 0s for TCP/SCTP | 0s for TCP/SCTP | |

## 7.8 IM CN subsystem timers

Table 7.9 shows recommended values for timers specific to the IM CN subsystem.

**Table 7.9: IM CN subsystem**

| Timer | Value to be applied at the UE | Value to be applied at the P-CSCF | Value to be applied at the S-CSCF | Meaning |
|---|---|---|---|---|
| reg-await-auth | not applicable | not applicable | 4 minutes | The timer is used by the S-CSCF during the authentication procedure of the UE. For detailed usage of the timer see subclause 5.4.1.2.<br>The authentication procedure may take in the worst case as long as 2 times Timer F. The IM CN subsystem value for Timer F is 128 seconds. |

NOTE: The UE and the P-CSCF use the value of the reg-await-auth timer to set the SIP level lifetime of the temporary set of security associations.

# 8 SIP compression

## 8.1 SIP compression procedures at the UE

### 8.1.1 SIP compression

The UE shall support SigComp as specified in RFC 3320 [32]. When using SigComp the UE shall send compressed SIP messages in accordance with RFC 3486 [55]. When the UE will create the compartment is implementation specific, but the compartment shall not be created until a set of security associations are set up. The compartment shall finish when the UE is deregistered. State creations and announcements shall be allowed only for messages received in a security association.

NOTE: Exchange of bytecodes during registration will prevent unnecessary delays during session setup.

Editor"s note: The draft-ietf-rohc-sigcomp-sip-01 [79] can lead to the need for additional changes or clarifications.

The UE shall support the SIP dictionary specified in RFC 3485 [42]. If compression is enabled, the UE shall use the dictionary to compress the first message.

The following apply when signalling compression is used:

- State Memory Size greater than zero is needed to give room for the UDVM byte code and make dynamic compression possible. A State Memory Size of at least 4096 bytes shall be a minimum value; and
- A Decompression Memory Size of at least 8192 bytes shall be a minimum value.

### 8.1.2 Compression of SIP requests and responses transmitted to the P-CSCF

The UE should compress the requests and responses transmitted to the P-CSCF according to subclause 8.1.1.

NOTE 1: Compression of SIP messages is an implementation option. However, compression is strongly recommended.

NOTE 2: Since compression support is mandatory, the UE may send even the first message compressed. Sigcomp provides mechanisms to allow the UE to know if state has been created in the P-CSCF or not.

### 8.1.3 Decompression of SIP requests and responses received from the P-CSCF

The UE shall decompress the compressed requests and responses received from the P-CSCF according to subclause 8.1.1.

If the UE detects a decompression failure at the P-CSCF, the recovery mechanism is implementation specific.

## 8.2 SIP compression procedures at the P-CSCF

### 8.2.1 SIP compression

The P-CSCF shall support SigComp as specified in RFC 3320 [32]. When using SigComp the P-CSCF shall send compressed SIP messages in accordance with RFC 3486 [55]. When the P-CSCF will create the compartment is implementation specific, but the compartment shall not be created until a set of security associations are set up. The compartment shall finish when the UE is deregistered. State creations and announcements shall be allowed only for messages received in a security association.

The P-CSCF shall support the SIP dictionary specified in RFC 3485 [42]. If compression is enabled, the P-CSCF shall use the dictionary to compress the first message.

NOTE: Exchange of bytecodes during registration will prevent unnecessary delays during session setup.

Editor"s note: The draft-ietf-rohc-sigcomp-sip-01 [79] can lead to the need for additional changes or clarifications.

The following apply when signalling compression is used:

- State Memory Size greater than zero is needed to give room for the UDVM byte code and make dynamic compression possible. A State Memory Size of at least 4096 bytes shall be a minimum value; and

- A Decompression Memory Size of at least 8192 bytes shall be a minimum value.

### 8.2.2 Compression of SIP requests and responses transmitted to the UE

The P-CSCF should compress the requests and responses transmitted to the UE according to subclause 8.2.1.

NOTE: Compression of SIP messages is an implementation option. However, compression is strongly recommended.

### 8.2.3 Decompression of SIP requests and responses received from the UE

The P-CSCF shall decompress the compressed requests and responses received from the UE according to subclause 8.2.1.

If the P-CSCF detects a decompression failure at the UE, the recovery mechanism is implementation specific.

# 9 IP-Connectivity Access Network aspects when connected to the IM CN subsystem

## 9.1 Introduction

A UE accessing the IM CN subsystem and the IM CN subsystem itself utilises the services supported by the IP-CAN to provide packet-mode communication between the UE and the IM CN subsystem. General requirements for the UE on the use of these packet-mode services are specified in this clause.

Possible aspects particular to each IP-CAN is described separately for each IP-CAN.

## 9.2 Procedures at the UE

### 9.2.1 Connecting to the IP-CAN and P-CSCF discovery

Prior to communication with the IM CN subsystem, the UE shall:

a) establish a connection with the IP-CAN;

b) obtain an IP address using either the standard IETF protocols (e.g., DHCP or IPCP) or a protocol that is particular to the IP-CAN technology that the UE is utilising. The obtained IP address shall be fixed throughout the period the UE is connected to the IM CN subsystem, i.e. from the initial registration and at least until the last deregistration; and

c) acquire a P-CSCF address(es).

The methods for acquiring a P-CSCF address(es) are:

I. Employ Dynamic Host Configuration Protocol for IPv6 (DHCPv6) RFC 3315 [40] and the DHCPv6 options for SIP servers RFC 3319 [41] and the DHCPv6 options for Domain Name Servers (DNS) RFC 3646 [56C].

The UE shall either:

- in the DHCP query, request a list of SIP server domain names of P-CSCF(s) and the list of Domain Name Servers (DNS); or

- request a list of SIP server IPv6 addresses of P-CSCF(s).

II. Obtain the P-CSCF address(es) by employing a procedure that the IP-CAN technology supports. (e.g. GPRS).

When acquiring a P-CSCF address(es) the UE can freely select either method I or II.

The UE may also request a DNS Server IPv6 address(es) as specified in RFC 3315 [40] and RFC 3646 [56C].

### 9.2.2 Handling of the IP-CAN

The UE shall ensure that appropriate resources are available for the media flow(s) on the IP-CAN(s) related to a SIP-session. The means to ensure this is dependant on the characteristics for each IP-CAN, and is described separately for each IP-CAN in question.

GPRS is described in annex B. I-WLAN is described in annex D.

### 9.2.3 Special requirements applying to forked responses

Since the UE does not know that forking has occurred until a second provisional response arrives, the UE will request the radio/bearer resources as required by the first provisional response. For each subsequent provisional response that may be received, different alternative actions may be performed depending on the requirements in the SDP answer:

- the UE has sufficient radio/bearer resources to handle the media specified in the SDP of the subsequent provisional response, or

- the UE must request additional radio/bearer resources to accommodate the media specified in the SDP of the subsequent provisional response.

NOTE 1: When several forked responses are received, the resources requested by the UE is the 'logical OR' of the resources indicated in the multiple responses to avoid allocation of unnecessary resources. The UE does not request more resources than proposed in the original INVITE request.

NOTE 2: When service-based local policy is applied, the UE receives the same authorization token for all forked requests/responses related to the same SIP session.

When a first final 200 (OK) response for the INVITE request is received for one of the early dialogues, the UE proceeds to set up the SIP session using the radio/bearer resources required for this session. Upon the reception of a first final 200 (OK) response for the INVITE request, the UE shall release all unneeded radio/bearer resources.

# Annex A (normative): Profiles of IETF RFCs for 3GPP usage

## A.1 Profiles

### A.1.1 Relationship to other specifications

This annex contains a profile to the IETF specifications which are referenced by this specification, and the PICS proformas underlying profiles do not add requirements to the specifications they are proformas for.

This annex provides a profile specification according to both the current IETF specifications for SIP, SDP and other protocols (as indicated by the "RFC status" column in the tables in this annex) which are referenced by this specification and to the 3GPP specifications using SIP (as indicated by the "Profile status" column in the tables in this annex.

In the "RFC status" column the contents of the referenced specification takes precedence over the contents of the entry in the column.

In the "Profile status" column, there are a number of differences from the "RFC status" column. Where these differences occur, these differences take precedence over any requirements of the IETF specifications. Where specification concerning these requirements exists in the main body of the present document, the main body of the present document takes precedence.

Where differences occur in the "Profile status" column, the "Profile status" normally gives more strength to a "RFC status" and is not in contradiction with the "RFC status", e.g. it may change an optional "RFC status" to a mandatory "Profile status". If the "Profile status" weakens the strength of a "RFC status" then additionally this will be indicated by further textual description in the present document.

For all IETF specifications that are not referenced by this document or that are not mentioned within the 3GPP profile of SIP and SDP, the generic rules as defined by RFC 3261 [26] and in addition the rules in clauses 5 and 6 of this specification apply, e.g..

- a proxy which is built in accordance to this specification passes on any unknown method, unknown header field or unknown header parameter after applying procedures such as filtering, insertion of P-Asserted-Identity header, etc.;

- an UA which is built in accordance to this specification will

  - handle received unknown methods in accordance to the procedures defined in RFC 3261 [26], e.g. respond with a 400 (Bad Request) response; and

  - handle unknown header fields and unknown header parameters in accordance to the procedures defined in RFC 3261 [26], e.g. respond with a 420 (Bad Extension) if an extension identified by an option tag in the Require header of the received request is not supported by the UA.

### A.1.2 Introduction to methodology within this profile

This subclause does not reflect dynamic conformance requirements but static ones. In particular, an condition for support of a PDU parameter does not reflect requirements about the syntax of the PDU (i.e. the presence of a parameter) but the capability of the implementation to support the parameter.

In the sending direction, the support of a parameter means that the implementation is able to send this parameter (but it does not mean that the implementation always sends it).

In the receiving direction, it means that the implementation supports the whole semantic of the parameter that is described in the main part of this specification.

As a consequence, PDU parameter tables in this subclause are not the same as the tables describing the syntax of a PDU in the reference specification, e.g. RFC 3261 [26] tables 2 and 3. It is not rare to see a parameter which is optional in the syntax but mandatory in subclause below.

The various statii used in this subclause are in accordance with the rules in table A.1.

**Table A.1: Key to status codes**

| Status code | Status name | Meaning |
|---|---|---|
| m | mandatory | the capability shall be supported. It is a static view of the fact that the conformance requirements related to the capability in the reference specification are mandatory requirements. This does not mean that a given behaviour shall always be observed (this would be a dynamic view), but that it shall be observed when the implementation is placed in conditions where the conformance requirements from the reference specification compel it to do so. For instance, if the support for a parameter in a sent PDU is mandatory, it does not mean that it shall always be present, but that it shall be present according to the description of the behaviour in the reference specification (dynamic conformance requirement). |
| o | optional | the capability may or may not be supported. It is an implementation choice. |
| n/a | not applicable | it is impossible to use the capability. No answer in the support column is required. |
| x | prohibited (excluded) | It is not allowed to use the capability. This is more common for a profile. |
| c <integer> | conditional | the requirement on the capability ("m", "o", "n/a" or "x") depends on the support of other **optional or conditional** items. <integer> is the identifier of the conditional expression. |
| o.<integer> | qualified optional | for mutually exclusive or selectable options from a set. <integer> is the identifier of the group of options, and the logic of selection of the options. |
| i | irrelevant | capability outside the scope of the given specification. Normally, this notation should be used in a base specification ICS proforma only for transparent parameters in received PDUs. However, it may be useful in other cases, when the base specification is in fact based on another standard. |

In the context of this specification the "i" status code mandates that the implementation does not change the content of the parameter. It is an implementation option if the implementation acts upon the content of the parameter (e.g. by setting filter criteria to known or unknown parts of parameters in order to find out the route a message has to take).

It must be understood, that this 3GPP SIP profile does not list all parameters which an implementation will treat as indicated by the status code "irrelevant". In general an implementation will pass on all unknown messages, header fields and header parameters, as long as it can perform its normal behaviour.

The following additional comments apply to the interpretation of the tables in this Annex.

NOTE 1: The tables are constructed according to the conventional rules for ICS proformas and profile tables.

NOTE 2: The notation (either directly or as part of a conditional) of "m" for the sending of a parameter and "i" for the receipt of the same parameter, may be taken as indicating that the parameter is passed on transparently, i.e. without modification. Where a conditional applies, this behaviour only applies when the conditional is met.

## A.1.3 Roles

**Table A.2: Roles**

| Item | Roles | Reference | RFC status | Profile status |
|---|---|---|---|---|
| 1 | User agent | [26] | o.1 | o.1 |
| 2 | Proxy | [26] | o.1 | o.1 |
| o.1: | It is mandatory to support exactly one of these items. | | | |
| NOTE: | For the purposes of the present document it has been chosen to keep the specification simple by the tables specifying only one role at a time. This does not preclude implementations providing two roles, but an entirely separate assessment of the tables shall be made for each role. | | | |

**Table A.3: Roles specific to this profile**

| Item | Roles | Reference | RFC status | Profile status |
|---|---|---|---|---|
| 1 | UE | 5.1 | n/a | o.1 |
| 2 | P-CSCF | 5.2 | n/a | o.1 |
| 3 | I-CSCF | 5.3 | n/a | o.1 |
| 3A | I-CSCF (THIG) | 5.3 | n/a | c1 |
| 4 | S-CSCF | 5.4 | n/a | o.1 |
| 5 | BGCF | 5.6 | n/a | o.1 |
| 6 | MGCF | 5.5 | n/a | o.1 |
| 7 | AS | 5.7 | n/a | o.1 |
| 7A | AS acting as terminating UA, or redirect server | 5.7.2 | n/a | c2 |
| 7B | AS acting as originating UA | 5.7.3 | n/a | c2 |
| 7C | AS acting as a SIP proxy | 5.7.4 | n/a | c2 |
| 7D | AS performing 3rd party call control | 5.7.5 | n/a | c2 |
| 8 | MRFC | 5.8 | n/a | o.1 |
| 9 | IMS-ALG | 5.9 | n/a | o.1 |
| c1: | IF A.3/3 THEN o ELSE x - - I-CSCF. | | | |
| c2: | IF A.3/7 THEN o.2 ELSE n/a - - AS. | | | |
| o.1: | It is mandatory to support exactly one of these items. | | | |
| o.2: | It is mandatory to support at least one of these items. | | | |
| NOTE: | For the purposes of the present document it has been chosen to keep the specification simple by the tables specifying only one role at a time. This does not preclude implementations providing two roles, but an entirely separate assessment of the tables shall be made for each role. | | | |

**Table A.3A: Roles specific to additional capabilities**

| Item | Roles | Reference | RFC status | Profile status |
|---|---|---|---|---|
| 1 | Presence server | 3GPP TS 24.141 [8A] | n/a | c1 |
| 2 | Presence user agent | 3GPP TS 24.141 [8A] | n/a | c2 |
| 3 | Resource list server | 3GPP TS 24.141 [8A] | n/a | c3 |
| 4 | Watcher | 3GPP TS 24.141 [8A] | n/a | c4 |
| 11 | Conference focus | 3GPP TS 24.147 [8B] | n/a | c5 |
| 12 | Conference participant | 3GPP TS 24.147 [8B] | n/a | c6 |
| c1: | IF A.3/7A AND A.3/7B THEN o ELSE n/a - - AS acting as terminating UA, or redirect server and AS acting as originating UA. | | | |
| c2: | IF A.3/1 THEN o ELSE n/a - - UE. | | | |
| c3: | IF A.3/7A THEN o ELSE n/a - - AS acting as terminating UA, or redirect server. | | | |
| c4: | IF A.3/1 OR A.3/7B THEN o ELSE IF A.3/9 THEN m ELSE n/a - - UE or AS acting as originating UA. | | | |
| c5: | IF A.3/7D AND A.3/4 AND A.3/8 THEN o ELSE n/a - - AS performing 3rd party call control and S-CSCF and MRFC (note 2). | | | |
| c6: | IF A.3/1 OR A.3A/11 THEN o ELSE IF A.3/9 THEN m ELSE n/a - - UE or conference focus. | | | |
| NOTE 1: | For the purposes of the present document it has been chosen to keep the specification simple by the tables specifying only one role at a time. This does not preclude implementations providing two roles, but an entirely separate assessment of the tables shall be made for each role. | | | |
| NOTE 2: | The functional split between the MRFC and the conferencing AS is out of scope of this document and they are assumed to be collocated. | | | |

# A.2 Profile definition for the Session Initiation Protocol as used in the present document

## A.2.1 User agent role

### A.2.1.1 Introduction

This subclause contains the ICS proforma tables related to the user role. They need to be completed only for UA implementations:

Prerequisite: A.2/1 - - user agent role.

### A.2.1.2 Major capabilities

**Table A.4: Major capabilities**

| Item | Does the implementation support | Reference | RFC status | Profile status |
|---|---|---|---|---|
| | **Capabilities within main protocol** | | | |
| 1 | client behaviour for registration? | [26] subclause 10.2 | o | c3 |
| 2 | registrar? | [26] subclause 10.3 | o | c4 |
| 2A | registration of multiple contacts for a single address of record | [26] 10.2.1.2, 16.6 | o | o |
| 2B | initiating a session? | [26] subclause 13 | o | o |
| 3 | client behaviour for INVITE requests? | [26] subclause 13.2 | c18 | c18 |
| 4 | server behaviour for INVITE requests? | [26] subclause 13.3 | c18 | c18 |
| 5 | session release? | [26] subclause 15.1 | c18 | c18 |
| 6 | timestamping of requests? | [26] subclause 8.2.6.1 | o | o |
| 7 | authentication between UA and UA? | [26] subclause 22.2 | c34 | c34 |
| 8 | authentication between UA and registrar? | [26] subclause 22.2 | o | n/a |
| 8A | authentication between UA and proxy? | [26] 20.28, 22.3 | o | o |
| 9 | server handling of merged requests due to forking? | [26] 8.2.2.2 | m | m |
| 10 | client handling of multiple responses due to forking? | [26] 13.2.2.4 | m | m |
| 11 | insertion of date in requests and responses? | [26] subclause 20.17 | o | o |
| 12 | downloading of alerting information? | [26] subclause 20.4 | o | o |
| | **Extensions** | | | |
| 13 | the SIP INFO method? | [25] | o | n/a |
| 14 | reliability of provisional responses in SIP? | [27] | c19 | c18 |
| 15 | the REFER method? | [36] | o | c33 |
| 16 | integration of resource management and SIP? | [30] [64] | c19 | c18 |
| 17 | the SIP UPDATE method? | [29] | c5 | c18 |
| 19 | SIP extensions for media authorization? | [31] | o | c14 |
| 20 | SIP specific event notification? | [28] | o | c13 |
| 21 | the use of NOTIFY to establish a dialog? | [28] 4.2 | o | n/a |
| 22 | acting as the notifier of event information? | [28] | c2 | c15 |
| 23 | acting as the subscriber to event information? | [28] | c2 | c16 |
| 24 | session initiation protocol extension header field for registering non-adjacent contacts? | [35] | o | c6 |
| 25 | private extensions to the Session Initiation Protocol (SIP) for network asserted identity within trusted networks? | [34] | o | m |
| 26 | a privacy mechanism for the Session Initiation Protocol (SIP)? | [33] | o | m |
| 26A | request of privacy by the inclusion of a Privacy header indicating any privacy option? | [33] | c9 | c11 |
| 26B | application of privacy based on the received Privacy header? | [33] | c9 | n/a |
| 26C | passing on of the Privacy header transparently? | [33] | c9 | c12 |
| 26D | application of the privacy option "header" such that those headers which cannot be completely expunged of identifying information without the assistance of intermediaries are obscured? | [33] 5.1 | c10 | c27 |
| 26E | application of the privacy option "session" such that anonymization for | [33] 5.2 | c10 | c27 |

| | | | | |
|---|---|---|---|---|
| | the session(s) initiated by this message occurs? | | | |
| 26F | application of the privacy option "user" such that user level privacy functions are provided by the network? | [33] 5.3 | c10 | c27 |
| 26G | application of the privacy option "id" such that privacy of the network asserted identity is provided by the network? | [34] 7 | c10 | n/a |
| 27 | a messaging mechanism for the Session Initiation Protocol (SIP)? | [50] | o | c7 |
| 28 | session initiation protocol extension header field for service route discovery during registration? | [38] | o | c17 |
| 29 | compressing the session initiation protocol? | [55] | o | c8 |
| 30 | private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP)? | [52] | o | m |
| 31 | the P-Associated-URI header extension? | [52] 4.1 | c21 | c22 |
| 32 | the P-Called-Party-ID header extension? | [52] 4.2 | c21 | c23 |
| 33 | the P-Visited-Network-ID header extension? | [52] 4.3 | c21 | c24 |
| 34 | the P-Access-Network-Info header extension? | [52] 4.4 | c21 | c25 |
| 35 | the P-Charging-Function-Addresses header extension? | [52] 4.5 | c21 | c26 |
| 36 | the P-Charging-Vector header extension? | [52] 4.6 | c21 | c26 |
| 37 | security mechanism agreement for the session initiation protocol? | [48] | o | c20 |
| 38 | the Reason header field for the session initiation protocol? | [34A] | o | o (note 1) |
| 39 | an extension to the session initiation protocol for symmetric response routeing? | [56A] | o | x |
| 40 | caller preferences for the session initiation protocol? | [56B] | C29 | c29 |
| 40A | the proxy-directive within caller-preferences? | [56B] 9.1 | o.5 | o.5 |
| 40B | the cancel-directive within caller-preferences? | [56B] 9.1 | o.5 | o.5 |
| 40C | the fork-directive within caller-preferences? | [56B] 9.1 | o.5 | c28 |
| 40D | the recurse-directive within caller-preferences? | [56B] 9.1 | o.5 | o.5 |
| 40E | the parallel-directive within caller-preferences? | [56B] 9.1 | o.5 | c28 |
| 40F | the queue-directive within caller-preferences? | [56B] 9.1 | o.5 | o.5 |
| 41 | an event state publication extension to the session initiation protocol? | [70] | o | c30 |
| 42 | SIP session timer? | [58] | c19 | c19 |
| 43 | the SIP Referred-By mechanism? | [59] | o | c33 |
| 44 | the Session Inititation Protocol (SIP) "Replaces" header? | [60] | c19 | c19 (note 1) |
| 45 | the Session Inititation Protocol (SIP) "Join" header? | [61] | c19 | c19 (note 1) |
| 46 | the callee capabilities? | [62] | o | c35 |

| | |
|---|---|
| c2: | IF A.4/20 THEN o.1 ELSE n/a - - SIP specific event notification extension. |
| c3: | IF A.3/1 OR A.3/4 THEN m ELSE n/a - - UE or S-CSCF functional entity. |
| c4: | IF A.3/4 THEN m ELSE IF A.3/7 THEN o ELSE n/a - - S-CSCF or AS functional entity. |
| c5: | IF A.4/16 THEN m ELSE o - - integration of resource management and SIP extension. |
| c6: | IF A.3/4 OR A.3/1 THEN m ELSE n/a. - - S-CSCF or UE. |
| c7: | IF A.3/1 OR A.3/4 OR A.3/7A OR A.3/7B OR A.3/7D OR A.3/9 THEN m ELSE n/a - - UA or S-CSCF or AS acting as terminating UA or AS acting as originating UA or AS performing 3rd party call control or IMS-ALG. |
| c8: | IF A.3/1 THEN m ELSE n/a - - UE behaviour. |
| c9: | IF A.4/26 THEN o.2 ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP). |
| c10: | IF A.4/26B THEN o.3 ELSE n/a - - application of privacy based on the received Privacy header. |
| c11: | IF A.3/1 OR A.3/6 THEN o ELSE IF A.3/9 THEN m ELSE n/a - - UE or MGCF, IMS-ALG. |
| c12: | IF A.3/7D THEN m ELSE n/a - - AS performing 3rd-party call control. |
| c13: | IF A.3/1 OR A.3/2 OR A.3/4 OR A.3/9 THEN m ELSE o - - UE or S-CSCF or IMS-ALG. |
| c14: | IF A.3/1 THEN m ELSE IF A.3/2 THEN o ELSE n/a – UE or P-CSCF. |
| c15: | IF A.4/20 AND (A.3/4 OR A.3/9) THEN m ELSE o – SIP specific event notification extensions and S-CSCF, IMS-ALG. |
| c16: | IF A.4/20 AND (A.3/1 OR A.3/2 OR A.3/9) THEN m ELSE o - - SIP specific event notification extension and UE or P-CSCF OR IMS-ALG. |
| c17: | IF A.3/1 or A.3/4 THEN m ELSE n/a - - UE or S-CSCF. |
| c18: | IF A.4/2B THEN m ELSE n/a - - initiating sessions. |
| c19: | IF A.4/2B THEN o ELSE n/a - - initiating sessions. |
| c20: | IF A.3/1 THEN m ELSE n/a - - UE behaviour. |
| c21: | IF A.4/30 THEN o.4 ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP). |
| c22: | IF A.4/30 AND (A.3/1 OR A.3/4) THEN m ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and S-CSCF or UA. |
| c23: | IF A.4/30 AND A.3/1 THEN o ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and UE. |
| c24: | IF A.4/30 AND A.3/4) THEN m ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and S-CSCF. |
| c25: | IF A.4/30 AND (A.3/1 OR A.3/4 OR A.3/7A OR A.3/7D OR A.3/9) THEN m ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and UE, S-CSCF or AS acting as terminating UA or AS acting as third-party call controller, IMS-ALG. |
| c26: | IF A.4/30 AND (A.3/6 OR A.3/7A OR A.3/7B or A.3/7D) THEN m ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and MGCF, AS acting as a terminating UA, or AS acting as an originating UA, or AS acting as third-party call controller. |
| c27: | IF A.3/7D THEN o ELSE x - - AS performing 3rd party call control. |
| c28: | IF A.3/1 THEN m ELSE o.5 - - UE. |
| c29: | IF A.4/40A OR A.4/40B OR A.4/40C OR A.4/40D OR A.4/40E OR A.4/40F THEN m ELSE n/a - - support of any directives within caller preferences for the session initiation protocol. |
| c30: | IF A.3A/1 OR A.3A/2 THEN m ELSE IF A.3/1 THEN o ELSE n/a - - presence server, presence user agent, UE, AS. |
| c33: | IF A.3/11 OR A.3/12 OR A.3/9 OR A.4/44 THEN m ELSE o - - conference focus or conference participant or IMS-ALG or the Session Inititation Protocol (SIP) "Replaces" header. |
| c34: | IF A.4/44 OR A.4/45 OR A.3/9 THEN m ELSE n/a - - the Session Inititation Protocol (SIP) "Replaces" header or the Session Inititation Protocol (SIP) "Join" header or IMS-ALG. |
| c35: | IF A.3/4 OR A.3/9 THEN m ELSE IF (A.3/1 OR A.3/6 OR A.3/7 OR A.3/8) THEN o ELSE n/a - - S-CSCF or IMS-ALG functional entities, UE or MGCF or AS or MRFC functional entity. |
| o.1: | At least one of these capabilities is supported. |
| o.2: | At least one of these capabilities is supported. |
| o.3: | At least one of these capabilities is supported. |
| o.4: | At least one of these capabilities is supported. |
| o.5: | At least one of these capabilities is supported. |
| NOTE 1: | At the MGCF, the interworking specifications do not support a handling of the header associated with this extension. |

Prerequisite A.5/20 - - SIP specific event notification

**Table A.4A: Supported event packages**

| Item | Does the implementation support | Subscriber | | | Notifier | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | reg event package? | [43] | c1 | c3 | [43] | c2 | c4 |
| 2 | refer package? | [36] 3 | c13 | c13 | [36] 3 | c13 | c13 |
| 3 | presence package? | [74] 6 | c1 | c5 | [74] 6 | c2 | c6 |
| 4 | eventlist with underlying presence package? | [75], [74] 6 | c1 | c7 | [75], [74] 6 | c2 | c8 |
| 5 | presence.winfo template-package? | [72] 4 | c1 | c9 | [72] 4 | c2 | c10 |
| 6 | ua-profile package? | [77] 3 | c1 | c11 | [77] 3 | c2 | c12 |
| 7 | conference package? | [78] 3 | c1 | c21 | [78] 3 | c1 | c22 |

c1: IF A.4/23 THEN o ELSE n/a - - acting as the subscriber to event information.
c2: IF A.4/22 THEN o ELSE n/a - - acting as the notifier of event information.
c3: IF A.3/1 OR A.3/2 THEN m ELSE IF A.3/7 THEN o ELSE n/a - - UE, P-CSCF, AS.
c4: IF A.3/4 THEN m ELSE n/a - - S-CSCF.
c5: IF A.3A/3 OR A.3A/4 THEN m ELSE IF A.4/23 THEN o ELSE n/a - - resource list server or watcher, acting as the subscriber to event information.
c6: IF A.3A/1 THEN m ELSE IF A.4/22 THEN o ELSE n/a - - presence server, acting as the notifier of event information.
c7: IF A.3A/4 THEN m ELSE IF A.4/23 THEN o ELSE n/a - - watcher, acting as the subscriber to event information.
c8: IF A.3A/3 THEN m ELSE IF A.4/22 THEN o ELSE n/a - - resource list server, acting as the notifier of event information.
c9: IF A.3A/2 THEN m ELSE IF A.4/23 THEN o ELSE n/a - - presence user agent, acting as the subscriber to event information.
c10: IF A.3A/1 THEN m ELSE IF A.4/22 THEN o ELSE n/a - - presence server, acting as the notifier of event information.
c11: IF A.3A/2 OR A.3A/4 THEN o ELSE IF A.4/23 THEN o ELSE n/a - - presence user agent or watcher, acting as the subscriber to event information.
c12: IF A.3A/1 OR A.3A/3 THEN m ELSE IF A.4/22 THEN o ELSE n/a - - presence server or resource list server, acting as the notifier of event information.
c13: IF A.4/15 THEN m ELSE n/a - - the REFER method.
c21: IF A.3A/12 THEN m ELSE IF A.4/23 THEN o ELSE n/a - - conference participant or acting as the subscriber to event information.
c22: IF A.3A/11 THEN m ELSE IF A.4/22 THEN o ELSE n/a - - conference focus or acting as the notifier of event information.

### A.2.1.3 PDUs

**Table A.5: Supported methods**

| Item | PDU | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | ACK request | [26] 13 | c10 | c10 | [26] 13 | c11 | c11 |
| 2 | BYE request | [26] 15.1 | c12 | c12 | [26] 15.1 | c12 | c12 |
| 3 | BYE response | [26] 15.1 | c12 | c12 | [26] 15.1 | c12 | c12 |
| 4 | CANCEL request | [26] 9 | m | m | [26] 9 | m | m |
| 5 | CANCEL response | [26] 9 | m | m | [26] 9 | m | m |
| 8 | INVITE request | [26] 13 | c10 | c10 | [26] 13 | c11 | c11 |
| 9 | INVITE response | [26] 13 | c11 | c11 | [26] 13 | c10 | c10 |
| 9A | MESSAGE request | [50] 4 | c7 | c7 | [50] 7 | c7 | c7 |
| 9B | MESSAGE response | [50] 4 | c7 | c7 | [50] 7 | c7 | c7 |
| 10 | NOTIFY request | [28] 8.1.2 | c4 | c4 | [28] 8.1.2 | c3 | c3 |
| 11 | NOTIFY response | [28] 8.1.2 | c3 | c3 | [28] 8.1.2 | c4 | c4 |
| 12 | OPTIONS request | [26] 11 | m | m | [26] 11 | m | m |
| 13 | OPTIONS response | [26] 11 | m | m | [26] 11 | m | m |
| 14 | PRACK request | [27] 6 | c5 | c5 | [27] 6 | c5 | c5 |
| 15 | PRACK response | [27] 6 | c5 | c5 | [27] 6 | c5 | c5 |
| 15A | PUBLISH request | [70] 11.1.3 | c20 | c20 | [70] 11.1.3 | c20 | c20 |
| 15B | PUBLISH response | [70] 11.1.3 | c20 | c20 | [70] 11.1.3 | c20 | c20 |
| 16 | REFER request | [36] 3 | c1 | c1 | [36] 3 | c1 | c1 |
| 17 | REFER response | [36] 3 | c1 | c1 | [36] 3 | c1 | c1 |
| 18 | REGISTER request | [26] 10 | c8 | c8 | [26] 10 | c9 | c9 |
| 19 | REGISTER response | [26] 10 | c9 | c9 | [26] 10 | c8 | c8 |
| 20 | SUBSCRIBE request | [28] 8.1.1 | c3 | c3 | [28] 8.1.1 | c4 | c4 |
| 21 | SUBSCRIBE response | [28] 8.1.1 | c4 | c4 | [28] 8.1.1 | c3 | c3 |
| 22 | UPDATE request | [29] 6.1 | c6 | c6 | [29] 6.2 | c6 | c6 |
| 23 | UPDATE response | [29] 6.2 | c6 | c6 | [29] 6.1 | c6 | c6 |

c1: IF A.4/15 THEN m ELSE n/a - - the REFER method extension.
c3: IF A.4/23 THEN m ELSE n/a - - recipient for event information.
c4: IF A.4/22 THEN m ELSE n/a - - notifier of event information.
c5: IF A.4/14 THEN m ELSE n/a - - reliability of provisional responses extension.
c6: IF A.4/17 THEN m ELSE n/a - - the SIP update method extension.
c7: IF A.4/27 THEN m ELSE n/a - - the SIP MESSAGE method.
c8: IF A.4/1 THEN m ELSE n/a - - client behaviour for registration.
c9: IF A.4/2 THEN m ELSE n/a - - registrar.
c10: IF A.4/3 THEN m ELSE n/a - - client behaviour for INVITE requests.
c11: IF A.4/4 THEN m ELSE n/a - - server behaviour for INVITE requests.
c12: IF A.4/5 THEN m ELSE n/a - - session release.
c20: IF A.4/41 THEN m ELSE n/a.

## A.2.1.4 PDU parameters

### A.2.1.4.1 Status-codes

**Table A.6: Supported status-codes**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | 100 (Trying) | [26] 21.1.1 | c21 | c21 | [26] 21.1.1 | c11 | c11 |
| 101 | 1xx response | [26] 21.1 | p21 | p21 | [26] 21.1 | p21 | p21 |
| 2 | 180 (Ringing) | [26] 21.1.2 | c2 | c2 | [26] 21.1.2 | c1 | c1 |
| 3 | 181 (Call Is Being Forwarded) | [26] 21.1.3 | c2 | c2 | [26] 21.1.3 | c1 | c1 |
| 4 | 182 (Queued) | [26] 21.1.4 | c2 | c2 | [26] 21.1.4 | c1 | c1 |
| 5 | 183 (Session Progress) | [26] 21.1.5 | c1 | c1 | [26] 21.1.5 | c1 | c1 |
| 102 | 2xx response | [26] 21.2 | p22 | p22 | [26] 21.1 | p22 | p22 |
| 6 | 200 (OK) | [26] 21.2.1 | m | m | [26] 21.2.1 | m | m |
| 7 | 202 (Accepted) | [28] 8.3.1 | c3 | c3 | [28] 8.3.1 | c3 | c3 |
| 103 | 3xx response | [26] 21.3 | p23 | p23 | [26] 21.1 | p23 | p23 |
| 8 | 300 (Multiple Choices) | [26] 21.3.1 | | | [26] 21.3.1 | | |
| 9 | 301 (Moved Permanently) | [26] 21.3.2 | | | [26] 21.3.2 | | |
| 10 | 302 (Moved Temporarily) | [26] 21.3.3 | | | [26] 21.3.3 | | |
| 11 | 305 (Use Proxy) | [26] 21.3.4 | | | [26] 21.3.4 | | |
| 12 | 380 (Alternative Service) | [26] 21.3.5 | | | [26] 21.3.5 | | |
| 104 | 4xx response | [26] 21.4 | p24 | p24 | [26] 21.4 | p24 | p24 |
| 13 | 400 (Bad Request) | [26] 21.4.1 | m | m | [26] 21.4.1 | m | m |
| 14 | 401 (Unauthorized) | [26] 21.4.2 | o | c12 | [26] 21.4.2 | m | m |
| 15 | 402 (Payment Required) | [26] 21.4.3 | n/a | n/a | [26] 21.4.3 | n/a | n/a |
| 16 | 403 (Forbidden) | [26] 21.4.4 | m | m | [26] 21.4.4 | m | m |
| 17 | 404 (Not Found) | [26] 21.4.5 | m | m | [26] 21.4.5 | m | m |
| 18 | 405 (Method Not Allowed) | [26] 21.4.6 | m | m | [26] 21.4.6 | m | m |
| 19 | 406 (Not Acceptable) | [26] 21.4.7 | m | m | [26] 21.4.7 | m | m |
| 20 | 407 (Proxy Authentication Required) | [26] 21.4.8 | o | o | [26] 21.4.8 | m | m |
| 21 | 408 (Request Timeout) | [26] 21.4.9 | m | m | [26] 21.4.9 | m | m |
| 22 | 410 (Gone) | [26] 21.4.10 | m | m | [26] 21.4.10 | m | m |
| 22A | 412 (Conditional Request Failed) | [70] 11.2.1 | c20 | c20 | [70] 11.2.1 | c20 | c20 |
| 23 | 413 (Request Entity Too Large) | [26] 21.4.11 | m | m | [26] 21.4.11 | m | m |
| 24 | 414 (Request-URI Too Large) | [26] 21.4.12 | m | m | [26] 21.4.12 | m | m |
| 25 | 415 (Unsupported Media Type) | [26] 21.4.13 | m | m | [26] 21.4.13 | m | m |
| 26 | 416 (Unsupported URI Scheme) | [26] 21.4.14 | m | m | [26] 21.4.14 | m | m |
| 27 | 420 (Bad Extension) | [26] 21.4.15 | m | c13 | [26] 21.4.15 | m | m |
| 28 | 421 (Extension Required) | [26] 21.4.16 | o | | [26] 21.4.16 | i | i |
| 28A | 422 (Session Interval Too Small) | [58] 6 | c7 | c7 | [58] 6 | c7 | c7 |
| 29 | 423 (Interval Too Brief) | [26] 21.4.17 | c4 | c4 | [26] 21.4.17 | m | m |
| 29A | 429 (Provide Referrer Identity) | [59] 5 | c8 | c8 | [59] 5 | c9 | c9 |
| 30 | 480 (Temporarily Unavailable) | [26] 21.4.18 | m | m | [26] 21.4.18 | m | m |
| 31 | 481 (Call/Transaction Does Not Exist) | [26] 21.4.19 | m | m | [26] 21.4.19 | m | m |
| 32 | 482 (Loop Detected) | [26] 21.4.20 | m | m | [26] 21.4.20 | m | m |
| 33 | 483 (Too Many Hops) | [26] 21.4.21 | m | m | [26] 21.4.21 | m | m |
| 34 | 484 (Address Incomplete) | [26] 21.4.22 | o | o | [26] 21.4.22 | m | m |
| 35 | 485 (Ambiguous) | [26] 21.4.23 | o | o | [26] 21.4.23 | m | m |
| 36 | 486 (Busy Here) | [26] 21.4.24 | m | m | [26] 21.4.24 | m | m |
| 37 | 487 (Request Terminated) | [26] 21.4.25 | m | m | [26] 21.4.25 | m | m |
| 38 | 488 (Not Acceptable Here) | [26] 21.4.26 | m | m | [26] 21.4.26 | m | m |

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 39 | 489 (Bad Event) | [28] 7.3.2 | c3 | c3 | [28] 7.3.2 | c3 | c3 |
| 40 | 491 (Request Pending) | [26] 21.4.27 | m | m | [26] 21.4.27 | m | m |
| 41 | 493 (Undecipherable) | [26] 21.4.28 | m | m | [26] 21.4.28 | m | m |
| 41A | 494 (Security Agreement Required) | [48] 2 | c5 | c5 | [48] 2 | c6 | c6 |
| 105 | 5xx response | [26] 21.5 | p25 | p25 | [26] 21.5 | p25 | p25 |
| 42 | 500 (Internal Server Error) | [26] 21.5.1 | m | m | [26] 21.5.1 | m | m |
| 43 | 501 (Not Implemented) | [26] 21.5.2 | m | m | [26] 21.5.2 | m | m |
| 44 | 502 (Bad Gateway) | [26] 21.5.3 | o | o | [26] 21.5.3 | m | m |
| 45 | 503 (Service Unavailable) | [26] 21.5.4 | m | m | [26] 21.5.4 | m | m |
| 46 | 504 (Server Time-out) | [26] 21.5.5 | m | m | [26] 21.5.5 | m | m |
| 47 | 505 (Version not supported) | [26] 21.5.6 | m | m | [26] 21.5.6 | m | m |
| 48 | 513 (Message Too Large) | [26] 21.5.7 | m | m | [26] 21.5.7 | m | m |
| 49 | 580 (Precondition Failure) | [30] 8 | | | [30] 8 | | |
| 106 | 6xx response | [26] 21.6 | p26 | p26 | [26] 21.6 | p26 | p26 |
| 50 | 600 (Busy Everywhere) | [26] 21.6.1 | m | m | [26] 21.6.1 | m | m |
| 51 | 603 (Decline) | [26] 21.6.2 | c10 | c10 | [26] 21.6.2 | m | m |
| 52 | 604 (Does Not Exist Anywhere) | [26] 21.6.3 | m | m | [26] 21.6.3 | m | m |
| 53 | 606 (Not Acceptable) | [26] 21.6.4 | m | m | [26] 21.6.4 | m | m |

c1: IF A.5/9 THEN m ELSE n/a - - INVITE response.
c2: IF A.5/9 THEN o ELSE n/a - - INVITE response.
c3: IF A.4/20 THEN m ELSE n/a - - SIP specific event notification extension.
c4: IF A.5/19 OR A.5/21 THEN m ELSE n/a - - REGISTER response or SUBSCRIBE response.
c5: IF A.4/37 AND A.4/2 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol and registrar.
c6: IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.
c7: IF A.4/42 AND (A.5/9 OR A.5/23) THEN m ELSE n/a - - the SIP session timer AND (INVITE response OR UPDATE response).
c8: IF A.4/43 AND A.5/17 THEN o ELSE n/a - - the SIP Referred-By mechanism and REFER response.
c9: IF A.4/43 AND A.5/17 THEN m ELSE n/a - - the SIP Referred-By mechanism and REFER response.
c10: IF A.4/44 THEN m ELSE o - - the Session Inititation Protocol (SIP) "Replaces" header.
c11: IF A.5/9 THE m ELSE n/a - - INVITE response (note 1).
c12: IF A.3/4 THEN m ELSE o - - S-CSCF.
c13: IF A.3/1 OR A.3/2 OR A.3/4 THEN m ELSE o - - UE, P-CSCF, S-CSCF.
c20: IF A.4/41 THEN m ELSE n/a - - an event state publication extension to the session initiation protocol.
c21: IF A.5/9 THEN o ELSE n/a - - INVITE response.
p21: A.6/2 OR A.6/3 OR A.6/4 OR A.6/5 - - 1xx response.
p22: A.6/6 OR A.6/7 - - 2xx response.
p23: A.6/8 OR A.6/9 OR A.6/10 OR A.6/11 OR A.6/12 OR A.6/13 - - 3xx response.
p24: A.6/14 OR A.6/15 OR A.6/16 OR A.6/17 OR A.6/18 OR A.6/19 OR A.6/20 OR A.6/21 OR A.6/22 OR A.6/22A OR A.6/23 OR A.6/24 OR A.6/25 OR A.6/26 OR A.6/27 OR A.6/28 OR A.6/28A OR A.6/29 OR A.6/29A OR A.6/30 OR A.6/31 OR A.6/32 OR A.6/33 OR A.6/34 OR A.6/35 OR A.6/36 OR A.6/436 OR A.6/38 OR A.6/39 OR A.6/40 OR A.6/41 OR A.6/41A. - 4xx response.
p25: A.6/42 OR A.6/43 OR A.6/44 OR A.6/45 OR A.6/46 OR A.6/47 OR A.6/48 OR A.6/49 - - 5xx response
p26: A.6/50 OR A.6/51 OR A.6/52 OR A.6/53 - - 6xx response.

NOTE 1: RFC 3261 [26] gives the status of this header for methods other than INVITE as SHOULD NOT.

### A.2.1.4.2 ACK method

Prerequisite A.5/1 – ACK request

**Table A.7: Supported headers within the ACK request**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Accept-Contact | [56B] 9.2 | c9 | c9 | [56B] 9.2 | c10 | c10 |
| 2 | Allow-Events | [28] 7.2.2 | c1 | c1 | [28] 7.2.2 | c2 | c2 |
| 3 | Authorization | [26] 20.7 | c3 | c3 | [26] 20.7 | c3 | c3 |
| 4 | Call-ID | [26] 20.8 | m | m | [26] 20.8 | m | m |
| 6 | Content-Disposition | [26] 20.11 | o | o | [26] 20.11 | m | m |
| 7 | Content-Encoding | [26] 20.12 | o | o | [26] 20.12 | m | m |
| 8 | Content-Language | [26] 20.13 | o | o | [26] 20.13 | m | m |
| 9 | Content-Length | [26] 20.14 | m | m | [26] 20.14 | m | m |
| 10 | Content-Type | [26] 20.15 | m | m | [26] 20.15 | m | m |
| 11 | Cseq | [26] 20.16 | m | m | [26] 20.16 | m | m |
| 12 | Date | [26] 20.17 | c4 | c4 | [26] 20.17 | m | m |
| 13 | From | [26] 20.20 | m | m | [26] 20.20 | m | m |
| 14 | Max-Forwards | [26] 20.22 | m | m | [26] 20.22 | n/a | n/a |
| 15 | MIME-Version | [26] 20.24 | o | o | [26] 20.24 | m | m |
| 15A | Privacy | [33] 4.2 | c6 | n/a | [33] 4.2 | c6 | n/a |
| 16 | Proxy-Authorization | [26] 20.28 | c5 | c5 | [26] 20.28 | n/a | n/a |
| 17 | Proxy-Require | [26] 20.29 | o | n/a | [26] 20.29 | n/a | n/a |
| 17A | Reason | [34A] 2 | c8 | c8 | [34A] 2 | c8 | c8 |
| 17B | Reject-Contact | [56B] 9.2 | c9 | c9 | [56B] 9.2 | c10 | c10 |
| 17C | Request-Disposition | [56B] 9.1 | c9 | c9 | [56B] 9.1 | c10 | c10 |
| 18 | Require | [26] 20.32 | o | o | [26] 20.32 | m | m |
| 19 | Route | [26] 20.34 | m | m | [26] 20.34 | n/a | n/a |
| 20 | Timestamp | [26] 20.38 | c7 | c7 | [26] 20.38 | m | m |
| 21 | To | [26] 20.39 | m | m | [26] 20.39 | m | m |
| 22 | User-Agent | [26] 20.41 | o | o | [26] 20.41 | m | m |
| 23 | Via | [26] 20.42 | m | m | [26] 20.42 | m | m |

c1: IF A.4/20 THEN o ELSE n/a - - SIP specific event notification extension.
c2: IF A.4/20 THEN m ELSE n/a - - SIP specific event notification extension.
c3: IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA.
c4: IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.
c5: IF A.4/8A THEN m ELSE n/a - - authentication between UA and proxy.
c6: IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c7: IF A.4/6 THEN o ELSE n/a - - timestamping of requests.
c8: IF A.4/38 THEN o ELSE n/a - - the Reason header field for the session initiation protocol.
c9: IF A.4/40 THEN o ELSE n/a - - caller preferences for the session initiation protocol.
c10: IF A.4/40 THEN m ELSE n/a - - caller preferences for the session initiation protocol.

Editor's note: Is the following table a suitable way of showing the contents of message bodies.

Prerequisite A.5/1 – ACK request

**Table A.8: Supported message bodies within the ACK request**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | | | | | | | |

### A.2.1.4.3 BYE method

Prerequisite A.5/2 - - BYE request

**Table A.9: Supported headers within the BYE request**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Accept | [26] 20.1 | o | o | [26] 20.1 | m | m |
| 1A | Accept-Contact | [56B] 9.2 | c18 | c18 | [56B] 9.2 | c22 | c22 |
| 2 | Accept-Encoding | [26] 20.2 | o | o | [26] 20.2 | m | m |
| 3 | Accept-Language | [26] 20.3 | o | o | [26] 20.3 | m | m |
| 3A | Allow | [26] 20.5 | o | o | [26] 20.5 | m | m |
| 4 | Allow-Events | [28] 7.2.2 | c1 | c1 | [28] 7.2.2 | c2 | c2 |
| 5 | Authorization | [26] 20.7 | c3 | c3 | [26] 20.7 | c3 | c3 |
| 6 | Call-ID | [26] 20.8 | m | m | [26] 20.8 | m | m |
| 7 | Content-Disposition | [26] 20.11 | o | o | [26] 20.11 | m | m |
| 8 | Content-Encoding | [26] 20.12 | o | o | [26] 20.12 | m | m |
| 9 | Content-Language | [26] 20.13 | o | o | [26] 20.13 | m | m |
| 10 | Content-Length | [26] 20.14 | m | m | [26] 20.14 | m | m |
| 11 | Content-Type | [26] 20.15 | m | m | [26] 20.15 | m | m |
| 12 | Cseq | [26] 20.16 | m | m | [26] 20.16 | m | m |
| 13 | Date | [26] 20.17 | c4 | c4 | [26] 20.17 | m | m |
| 14 | From | [26] 20.20 | m | m | [26] 20.20 | m | m |
| 15 | Max-Forwards | [26] 20.22 | m | m | [26] 20.22 | n/a | n/a |
| 16 | MIME-Version | [26] 20.24 | o | o | [26] 20.24 | m | m |
| 16A | P-Access-Network-Info | [52] 4.4 | c9 | c10 | [52] 4.4 | c9 | c11 |
| 16B | P-Asserted-Identity | [34] 9.1 | n/a | n/a | [34] 9.1 | c6 | c6 |
| 16C | P-Charging-Function-Addresses | [52] 4.5 | c13 | c14 | [52] 4.5 | c13 | c14 |
| 16D | P-Charging-Vector | [52] 4.6 | c12 | n/a | [52] 4.6 | c12 | n/a |
| 16E | P-Preferred-Identity | [34] 9.2 | c6 | x | [34] 9.2 | n/a | n/a |
| 16F | Privacy | [33] 4.2 | c7 | n/a | [33] 4.2 | c7 | c7 |
| 17 | Proxy-Authorization | [26] 20.28 | c5 | c5 | [26] 20.28 | n/a | n/a |
| 18 | Proxy-Require | [26] 20.29 | o | n/a | [26] 20.29 | n/a | n/a |
| 18A | Reason | [34A] 2 | c17 | c17 | [34A] 2 | c17 | c17 |
| 19 | Record-Route | [26] 20.30 | n/a | n/a | [26] 20.30 | n/a | n/a |
| 19A | Referred-By | [59] 3 | c19 | c19 | [59] 3 | c20 | c20 |
| 19B | Reject-Contact | [56B] 9.2 | c18 | c18 | [56B] 9.2 | c22 | c22 |
| 19C | Request-Disposition | [56B] 9.1 | c18 | c18 | [56B] 9.1 | c22 | c22 |
| 20 | Require | [26] 20.32 | o | o | [26] 20.32 | m | m |
| 21 | Route | [26] 20.34 | m | m | [26] 20.34 | n/a | n/a |
| 21A | Security-Client | [48] 2.3.1 | c15 | c15 | [48] 2.3.1 | n/a | n/a |
| 21B | Security-Verify | [48] 2.3.1 | c16 | c16 | [48] 2.3.1 | n/a | n/a |
| 22 | Supported | [26] 20.37 | o | o | [26] 20.37 | m | m |
| 23 | Timestamp | [26] 20.38 | c8 | c8 | [26] 20.38 | m | m |
| 24 | To | [26] 20.39 | m | m | [26] 20.39 | m | m |
| 25 | User-Agent | [26] 20.41 | o | o | [26] 20.41 | o | o |
| 26 | Via | [26] 20.42 | m | m | [20] 20.42 | m | m |

| | |
|---|---|
| c1: | IF A.4/20 THEN o ELSE n/a - - SIP specific event notification extension. |
| c2: | IF A.4/20 THEN m ELSE n/a - - SIP specific event notification extension. |
| c3: | IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA. |
| c4: | IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses. |
| c5: | IF A.4/8A THEN m ELSE n/a - - authentication between UA and proxy. |
| c6: | IF A.4/25 THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks. |
| c7: | IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP). |
| c8: | IF A.4/6 THEN o ELSE n/a - - timestamping of requests. |
| c9: | IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension. |
| c10: | IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE. |
| c11: | IF A.4/34 AND (A.3/7A OR A.3/7D) THEN m ELSE n/a - - the P-Access-Network-Info header extension and AS acting as terminating UA or AS acting as third-party call controller. |
| c12: | IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension. |
| c13: | IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension. |
| c14: | IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension. |
| c15: | IF A.4/37 THEN o ELSE n/a - - security mechanism agreement for the session initiation protocol (note). |
| c16: | IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. |
| c17: | IF A.4/38 THEN o ELSE n/a - - the Reason header field for the session initiation protocol. |
| c18: | IF A.4/40 THEN o ELSE n/a - - caller preferences for the session initiation protocol. |
| c19: | IF A.4/43 THEN m ELSE n/a - - the SIP Referred-By mechanism. |
| c20: | IF A.4/43 THEN o ELSE n/a - - the SIP Referred-By mechanism. |
| c22: | IF A.4/40 THEN m ELSE n/a - - caller preferences for the session initiation protocol. |
| NOTE: | Support of this header in this method is dependent on the security mechanism and the security architecture which is implemented. Use of this header in this method is not appropriate to the security mechanism defined by 3GPP TS 33.203 [19]. |

Prerequisite A.5/2 - - BYE request

**Table A.10: Supported message bodies within the BYE request**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | | | | | | | |

**Table A.11: Void**

Prerequisite A.5/3 - - BYE response for all status-codes

**Table A.12: Supported headers within the BYE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 0A | Allow | [26] 20.5 | c11 | c11 | [26] 20.5 | m | m |
| 1 | Call-ID | [26] 20.8 | m | m | [26] 20.8 | m | m |
| 2 | Content-Disposition | [26] 20.11 | o | o | [26] 20.11 | m | m |
| 3 | Content-Encoding | [26] 20.12 | o | o | [26] 20.12 | m | m |
| 4 | Content-Language | [26] 20.13 | o | o | [26] 20.13 | m | m |
| 5 | Content-Length | [26] 20.14 | m | m | [26] 20.14 | m | m |
| 6 | Content-Type | [26] 20.15 | m | m | [26] 20.15 | m | m |
| 7 | Cseq | [26] 20.16 | m | m | [26] 20.16 | m | m |
| 8 | Date | [26] 20.17 | c1 | c1 | [26] 20.17 | m | m |
| 9 | From | [26] 20.20 | m | m | [26] 20.20 | m | m |
| 10 | MIME-Version | [26] 20.24 | o | o | [26] 20.24 | m | m |
| 10A | P-Access-Network-Info | [52] 4.4 | c5 | c6 | [52] 4.4 | c5 | c6 |
| 10B | P-Asserted-Identity | [34] 9.1 | n/a | n/a | [34] 9.1 | c3 | c3 |
| 10C | P-Charging-Function-Addresses | [52] 4.5 | c9 | c10 | [52] 4.5 | c9 | c10 |
| 10D | P-Charging-Vector | [52] 4.6 | c8 | n/a | [52] 4.6 | c8 | n/a |
| 10E | P-Preferred-Identity | [34] 9.2 | c3 | x | [34] 9.2 | n/a | n/a |
| 10F | Privacy | [33] 4.2 | c4 | n/a | [33] 4.2 | c4 | c4 |
| 10G | Require | [26] 20.32 | o | o | [26] 20.32 | m | m |
| 10H | Server | [26] 20.35 | o | o | [26] 20.35 | o | o |
| 11 | Timestamp | [26] 20.38 | m | m | [26] 20.38 | c2 | c2 |
| 12 | To | [26] 20.39 | m | m | [26] 20.39 | m | m |
| 12A | User-Agent | [26] 20.41 | o | o | [26] 20.41 | o | o |
| 13 | Via | [26] 20.42 | m | m | [26] 20.42 | m | m |
| 14 | Warning | [26] 20.43 | o (note) | o (note) | [26] 20.43 | o | o |

c1: IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.
c2: IF A.4/6 THEN m ELSE n/a - - timestamping of requests.
c3: IF A.4/25 THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.
c4: IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c5: IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.
c6: IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE.
c7: IF A.4/34 AND (A.3/7A OR A.3/7D) THEN m ELSE n/a - - the P-Access-Network-Info header extension and AS acting as terminating UA or AS acting as third-party call controller.
c8: IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.
c9: IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.
c10: IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.
c11: IF A.6/18 THEN m ELSE o - - 405 (Method Not Allowed)

NOTE: For a 488 (Not Acceptable Here) response, RFC 3261 [26] gives the status of this header as SHOULD rather than OPTIONAL.

Prerequisite A.5/3 - - BYE response

Prerequisite: A.6/102 - - Additional for 2xx response

**Table A.13: Supported headers within the BYE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 0A | Allow-Events | [28] 7.2.2 | c3 | c3 | [28] 7.2.2 | c4 | c4 |
| 1 | Authentication-Info | [26] 20.6 | c1 | c1 | [26] 20.6 | c2 | c2 |
| 4 | Supported | [26] 20.37 | o | m | [26] 20.37 | m | m |

| | |
|---|---|
| c1: | IF A.4/7 THEN o ELSE n/a - - authentication between UA and UA. |
| c2: | IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA. |
| c3: | IF A.4/20 THEN o ELSE n/a - - SIP specific event notification extension. |
| c4: | IF A.4/20 THEN m ELSE n/a - - SIP specific event notification extension. |

Prerequisite A.5/3 - - BYE response

Prerequisite: A.6/103 OR A.6/104 OR A.6/105 OR A.6/106 - - Additional for 3xx – 6xx response

**Table A.13A: Supported headers within the BYE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Error-Info | [26] 20.18 | o | o | [26] 20.18 | o | o |

Prerequisite A.5/3 - - BYE response

Prerequisite: A.6/103 OR A.6/35 - - Additional for 3xx or 485 (Ambiguous) response

**Table A.14: Supported headers within the BYE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 0B | Contact | [26] 20.10 | o (note) | o | [26] 20.10 | m | m |
| NOTE: | RFC 3261 [26] gives the status of this header as SHOULD rather than OPTIONAL. | | | | | | |

Prerequisite A.5/3 - - BYE response

Prerequisite: A.6/14 - - Additional for 401 (Unauthorized) response

**Table A.15: Supported headers within the BYE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 2 | Proxy-Authenticate | [26] 20.27 | c1 | c1 | [26] 20.27 | c1 | c1 |
| 8 | WWW-Authenticate | [26] 20.44 | m | m | [26] 20.44 | m | m |
| c1: | IF A.5/7 THEN m ELSE n/a - - support of authentication between UA and UA. | | | | | | |

Prerequisite A.5/3 - - BYE response

Prerequisite: A.6/17 OR A.6/23 OR A.6/30 OR A.6/36 OR A.6/42 OR A.6/45 OR A.6/50 OR A.6/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response

**Table A.16: Supported headers within the BYE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 3 | Retry-After | [26] 20.33 | o | o | [26] 20.33 | o | o |

**Table A.17: Void**

Prerequisite A.5/3 - - BYE response

Prerequisite: A.6/19 - - Additional for 407 (Proxy Authentication Required) response

**Table A.18: Supported headers within the BYE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 2 | Proxy-Authenticate | [26] 20.27 | c1 | c1 | [26] 20.27 | c1 | c1 |
| 6 | WWW-Authenticate | [26] 20.44 | o | o | [26] 20.44 | o | o |
| c1: | IF A.5/7 THEN m ELSE n/a - - support of authentication between UA and UA. | | | | | | |

Prerequisite A.5/3 - - BYE response

Prerequisite A.6/25 - - Additional for 415 (Unsupported Media Type) response

**Table A.19: Supported headers within the BYE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Accept | [26] 20.1 | o.1 | o.1 | [26] 20.1 | m | m |
| 2 | Accept-Encoding | [26] 20.2 | o.1 | o.1 | [26] 20.2 | m | m |
| 3 | Accept-Language | [26] 20.3 | o.1 | o.1 | [26] 20.3 | m | m |
| o.1 | At least one of these capabilities is supported. | | | | | | |

Prerequisite A.5/3 - - BYE response

Prerequisite: A.6/27 - - Additional for 420 (Bad Extension) response

**Table A.20: Supported headers within the BYE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 5 | Unsupported | [26] 20.40 | m | m | [26] 20.40 | m | m |

Prerequisite A.5/3 - - BYE response

Prerequisite: A.6/28 OR A.6/41A - - Additional for 421 (Extension Required), 494 (Security Agreement Required) response

**Table A.20A: Supported headers within the BYE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 3 | Security-Server | [48] 2 | x | x | [48] 2 | c1 | c1 |
| c1: | IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. | | | | | | |

**Table A.21: Void**

Prerequisite A.5/3 - - BYE response

**Table A.22: Supported message bodies within the BYE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | | | | | | | |

### A.2.1.4.4 CANCEL method

Prerequisite A.5/4 - - CANCEL request

**Table A.23: Supported headers within the CANCEL request**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Accept-Contact | [56B] 9.2 | c9 | c9 | [56B] 9.2 | c11 | c11 |
| 5 | Authorization | [26] 20.7 | c3 | c3 | [26] 20.7 | c3 | c3 |
| 6 | Call-ID | [26] 20.8 | m | m | [26] 20.8 | m | m |
| 8 | Content-Length | [26] 20.14 | m | m | [26] 20.14 | m | m |
| 9 | Cseq | [26] 20.16 | m | m | [26] 20.16 | m | m |
| 10 | Date | [26] 20.17 | c4 | c4 | [26] 20.17 | m | m |
| 11 | From | [26] 20.20 | m | m | [26] 20.20 | m | m |
| 12 | Max-Forwards | [26] 20.22 | m | m | [26] 20.22 | n/a | n/a |
| 14 | Privacy | [33] 4.2 | c6 | n/a | [33] 4.2 | c6 | n/a |
| 15 | Reason | [34A] 2 | c7 | c7 | [34A] 2 | c7 | c7 |
| 16 | Record-Route | [26] 20.30 | n/a | n/a | [26] 20.30 | n/a | n/a |
| 17 | Reject-Contact | [56B] 9.2 | c9 | c9 | [56B] 9.2 | c11 | c11 |
| 17A | Request-Disposition | [56B] 9.1 | c9 | c9 | [56B] 9.1 | c11 | c11 |
| 18 | Route | [26] 20.34 | m | m | [26] 20.34 | n/a | n/a |
| 19 | Supported | [26] 20.37 | o | o | [26] 20.37 | m | m |
| 20 | Timestamp | [26] 20.38 | c8 | c8 | [26] 20.38 | m | m |
| 21 | To | [26] 20.39 | m | m | [26] 20.39 | m | m |
| 22 | User-Agent | [26] 20.41 | o | | [26] 20.41 | o | |
| 23 | Via | [26] 20.42 | m | m | [26] 20.42 | m | m |
| c3: | IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA. | | | | | | |
| c4: | IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses. | | | | | | |
| c6: | IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP). | | | | | | |
| c7: | IF A.4/38 THEN o ELSE n/a - - the Reason header field for the session initiation protocol. | | | | | | |
| c8: | IF A.4/6 THEN o ELSE n/a - - timestamping of requests. | | | | | | |
| c9: | IF A.4/40 THEN o ELSE n/a - - caller preferences for the session initiation protocol. | | | | | | |
| c11: | IF A.4/40 THEN m ELSE n/a - - caller preferences for the session initiation protocol. | | | | | | |

Prerequisite A.5/4 - - CANCEL request

**Table A.24: Supported message bodies within the CANCEL request**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | | | | | | | |

Prerequisite A.5/5 - - CANCEL response for all status-codes

**Table A.25: Supported headers within the CANCEL response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Call-ID | [26] 20.8 | m | m | [26] 20.8 | m | m |
| 2 | Content-Length | [26] 20.14 | m | m | [26] 20.14 | m | m |
| 3 | Cseq | [26] 20.16 | m | m | [26] 20.16 | m | m |
| 4 | Date | [26] 20.17 | c1 | c1 | [26] 20.17 | m | m |
| 5 | From | [26] 20.20 | m | m | [26] 20.20 | m | m |
| 5A | Privacy | [33] 4.2 | c3 | n/a | [33] 4.2 | c3 | n/a |
| 6 | Timestamp | [26] 20.38 | m | m | [26] 20.38 | c2 | c2 |
| 7 | To | [26] 20.39 | m | m | [26] 20.39 | m | m |
| 7A | User-Agent | [26] 20.41 | o | o | [26] 20.41 | o | o |
| 8 | Via | [26] 20.42 | m | m | [26] 20.42 | m | m |
| 9 | Warning | [26] 20.43 | o (note) | o | [26] 20.43 | o | o |
| c1: | IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses. | | | | | | |
| c2: | IF A.4/6 THEN m ELSE n/a - - timestamping of requests. | | | | | | |
| c3: | IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP). | | | | | | |
| NOTE: | For a 488 (Not Acceptable Here) response, RFC 3261 [26] gives the status of this header as SHOULD rather than OPTIONAL. | | | | | | |

Prerequisite A.5/5 - - CANCEL response

Prerequisite: A.6/102 - - Additional for 2xx response

**Table A.26: Supported headers within the CANCEL response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 2 | Record-Route | [26] 20.30 | n/a | n/a | [26] 20.30 | n/a | n/a |
| 4 | Supported | [26] 20.37 | o | m | [26] 20.37 | m | m |

Prerequisite A.5/5 - - CANCEL response

Prerequisite: A.6/103 OR A.6/104 OR A.6/105 OR A.6/106 - - Additional for 3xx – 6xx response

**Table A.26A: Supported headers within the CANCEL response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Error-Info | [26] 20.18 | o | o | [26] 20.18 | o | o |

**Table A.27: Void**

Prerequisite A.5/5 - - CANCEL response

Prerequisite: A.6/17 OR A.6/23 OR A.6/30 OR A.6/42 OR A.6/45 OR A.6/50 OR A.6/51 - - Additional for Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response

**Table A.28: Supported headers within the CANCEL response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 4 | Retry-After | [26] 20.33 | o | o | [26] 20.33 | o | o |

**Table A.30: Void**

Prerequisite A.5/5 - - CANCEL response

**Table A.31: Supported message bodies within the CANCEL response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | | | | | | | |

### A.2.1.4.5 COMET method

Void

### A.2.1.4.6 INFO method

Void

### A.2.1.4.7 INVITE method

Prerequisite A.5/8 - - INVITE request

**Table A.46: Supported headers within the INVITE request**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Accept | [26] 20.1 | o | o | [26] 20.1 | m | m |
| 1A | Accept-Contact | [56B] 9.2 | c24 | c24 | [56B] 9.2 | c32 | c32 |
| 2 | Accept-Encoding | [26] 20.2 | o | o | [26] 20.2 | m | m |
| 3 | Accept-Language | [26] 20.3 | o | o | [26] 20.3 | m | m |
| 4 | Alert-Info | [26] 20.4 | o | o | [26] 20.4 | c1 | c1 |
| 5 | Allow | [26] 20.5, [26] 5.1 | o (note 1) | o | [26] 20.5, [26] 5.1 | m | m |
| 6 | Allow-Events | [28] 7.2.2 | c2 | c2 | [28] 7.2.2 | c2 | c2 |
| 8 | Authorization | [26] 20.7 | c3 | c3 | [26] 20.7 | c3 | c3 |
| 9 | Call-ID | [26] 20.8 | m | m | [26] 20.8 | m | m |
| 10 | Call-Info | [26] 20.9 | o | o | [26] 20.9 | o | o |
| 11 | Contact | [26] 20.10 | m | m | [26] 20.10 | m | m |
| 12 | Content-Disposition | [26] 20.11 | o | o | [26] 20.11 | m | m |
| 13 | Content-Encoding | [26] 20.12 | o | o | [26] 20.12 | m | m |
| 14 | Content-Language | [26] 20.13 | o | o | [26] 20.13 | m | m |
| 15 | Content-Length | [26] 20.14 | m | m | [26] 20.14 | m | m |
| 16 | Content-Type | [26] 20.15 | m | m | [26] 20.15 | m | m |
| 17 | Cseq | [26] 20.16 | m | m | [26] 20.16 | m | m |
| 18 | Date | [26] 20.17 | c4 | c4 | [26] 20.17 | m | m |
| 19 | Expires | [26] 20.19 | o | o | [26] 20.19 | o | o |
| 20 | From | [26] 20.20 | m | m | [26] 20.20 | m | m |
| 21 | In-Reply-To | [26] 20.21 | o | o | [26] 20.21 | o | o |
| 21A | Join | [61] 7.1 | c30 | c30 | [61] 7.1 | c30 | c30 |
| 22 | Max-Forwards | [26] 20.22 | m | m | [26] 20.22 | n/a | n/a |
| 23 | MIME-Version | [26] 20.24 | o | o | [26] 20.24 | m | m |
| 23A | Min-SE | [58] 5 | c26 | c26 | [58] 5 | c25 | c25 |
| 24 | Organization | [26] 20.25 | o | o | [26] 20.25 | o | o |
| 24A | P-Access-Network-Info | [52] 4.4 | c15 | c16 | [52] 4.4 | c15 | c17 |
| 24B | P-Asserted-Identity | [34] 9.1 | n/a | n/a | [34] 9.1 | c7 | c7 |
| 24C | P-Called-Party-ID | [52] 4.2 | x | x | [52] 4.2 | c13 | c13 |
| 24D | P-Charging-Function-Addresses | [52] 4.5 | c20 | c21 | [52] 4.5 | c20 | c21 |
| 24E | P-Charging-Vector | [52] 4.6 | c18 | c19 | [52] 4.6 | c18 | c19 |
| 25 | P-Media-Authorization | [31] 5.1 | n/a | n/a | [31] 5.1 | c11 | c12 |
| 25A | P-Preferred-Identity | [34] 9.2 | c7 | c5 | [34] 9.2 | n/a | n/a |
| 25B | P-Visited-Network-ID | [52] 4.3 | x (note 3) | x | [52] 4.3 | c14 | n/a |
| 26 | Priority | [26] 20.26 | o | o | [26] 20.26 | o | o |
| 26A | Privacy | [33] 4.2 | c9 | c9 | [33] 4.2 | c9 | c9 |
| 27 | Proxy-Authorization | [26] 20.28 | c6 | c6 | [26] 20.28 | n/a | n/a |
| 28 | Proxy-Require | [26] 20.29 | o (note 2) | o (note 2) | [26] 20.29 | n/a | n/a |
| 28A | Reason | [34A] 2 | c8 | c8 | [34A] 2 | c8 | c8 |
| 29 | Record-Route | [26] 20.30 | n/a | n/a | [26] 20.30 | m | m |
| 30 | Referred-By | [59] 3 | c27 | c27 | [59] 3 | c28 | c28 |
| 31 | Reject-Contact | [56B] 9.2 | c24 | c24 | [56B] 9.2 | c32 | c32 |
| 31A | Replaces | [60] 6.1 | c29 | c29 | [60] 6.1 | c29 | c29 |
| 31B | Reply-To | [26] 20.31 | o | o | [26] 20.31 | o | o |
| 31B | Request-Disposition | [56B] 9.1 | c24 | c24 | [56B] 9.1 | c32 | c32 |

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 32 | Require | [26] 20.32 | o | m | [26] 20.32 | m | m |
| 33 | Route | [26] 20.34 | m | m | [26] 20.34 | n/a | n/a |
| 33A | Security-Client | [48] 2.3.1 | c22 | c22 | [48] 2.3.1 | n/a | n/a |
| 33B | Security-Verify | [48] 2.3.1 | c23 | c23 | [48] 2.3.1 | n/a | n/a |
| 33C | Session-Expires | [58] 4 | c25 | c25 | [58] 4 | c25 | c25 |
| 34 | Subject | [26] 20.36 | o | o | [26] 20.36 | o | o |
| 35 | Supported | [26] 20.37 | m | m | [26] 20.37 | m | m |
| 36 | Timestamp | [26] 20.38 | c10 | c10 | [26] 20.38 | m | m |
| 37 | To | [26] 20.39 | m | m | [26] 20.39 | m | m |
| 38 | User-Agent | [26] 20.41 | o | o | [26] 20.41 | o | o |
| 39 | Via | [26] 20.42 | m | m | [26] 20.42 | m | m |

c1: IF A.4/12 THEN m ELSE n/a - - downloading of alerting information.
c2: IF A.4/20 THEN m ELSE n/a - - SIP specific event notification extension.
c3: IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA.
c4: IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.
c5: IF A.3/1 AND A.4/25 THEN o ELSE n/a - - UE and private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.
c6: IF A.4/8A THEN m ELSE n/a - - authentication between UA and proxy.
c7: IF A.4/25 THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.
c8: IF A.4/38 THEN o ELSE n/a - - the Reason header field for the session initiation protocol.
c9: IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c10: IF A.4/6 THEN o ELSE n/a - - timestamping of requests.
c11: IF A.4/19 THEN m ELSE n/a - - SIP extensions for media authorization.
c12: IF A.3/1 THEN m ELSE n/a - - UE.
c13: IF A.4/32 THEN o ELSE n/a - - the P-Called-Party-ID extension.
c14: IF A.4/33 THEN o ELSE n/a - - the P-Visited-Network-ID extension.
c15: IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.
c16: IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE.
c17: IF A.4/34 AND (A.3/7A OR A.3/7D) THEN m ELSE n/a - - the P-Access-Network-Info header extension and AS acting as terminating UA or AS acting as third-party call controller.
c18: IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.
c19: IF A.4/36 THEN m ELSE n/a - - the P-Charging-Vector header extension.
c20: IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.
c21: IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.
c22: IF A.4/37 THEN o ELSE n/a - - security mechanism agreement for the session initiation protocol (note 4).
c23: IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.
c24: IF A.4/40 THEN o ELSE n/a - - caller preferences for the session initiation protocol.
c25: IF A.4/42 THEN m ELSE n/a - - the SIP session timer.
c26: IF A.4/42 THEN o ELSE n/a - - the SIP session timer.
c27: IF A.4/43 THEN m ELSE n/a - - the SIP Referred-By mechanism.
c28: IF A.4/43 THEN o ELSE n/a - - the SIP Referred-By mechanism.
c29: IF A.4/44 THEN m ELSE n/a - - the Session Inititation Protocol (SIP) "Replaces" header.
c30: IF A.4/45 THEN m ELSE n/a - - the Session Inititation Protocol (SIP) "Join" header.
c32: IF A.4/40 THEN m ELSE n/a - - caller preferences for the session initiation protocol.
o.1: At least one of these shall be supported.

NOTE 1: RFC 3261 [26] gives the status of this header as SHOULD rather than OPTIONAL.
NOTE 2: No distinction has been made in these tables between first use of a request on a From/To/Call-ID combination, and the usage in a subsequent one. Therefore the use of "o" etc. above has been included from a viewpoint of first usage.
NOTE 3: The strength of this requirement in RFC 3455 [52] is SHOULD NOT, rather than MUST NOT.
NOTE 4: Support of this header in this method is dependent on the security mechanism and the security architecture which is implemented. Use of this header in this method is not appropriate to the security mechanism defined by 3GPP TS 33.203 [19].

Prerequisite A.5/8 - - INVITE request

**Table A.47: Supported message bodies within the INVITE request**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | | | | | | | |

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/1 - - Additional for 100 (Trying) response

**Table A.48: Supported headers within the INVITE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Call-ID | [26] 20.8 | m | m | [26] 20.8 | m | m |
| 2 | Content-Length | [26] 20.14 | m | m | [26] 20.14 | m | m |
| 3 | Cseq | [26] 20.16 | m | m | [26] 20.16 | m | m |
| 4 | Date | [26] 20.17 | c1 | c1 | [26] 20.17 | m | m |
| 5 | From | [26] 20.20 | m | m | [26] 20.20 | m | m |
| 6 | To | [26] 20.39 | m | m | [26] 20.39 | m | m |
| 7 | Via | [26] 20.42 | m | m | [26] 20.42 | m | m |
| c1: | IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses. | | | | | | |

Prerequisite A.5/9 - - INVITE response for all remaining status-codes

**Table A.49: Supported headers within the INVITE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 0A | Allow | [26] 20.5 | c12 | c12 | [26] 20.5 | m | m |
| 1 | Call-ID | [26] 20.8 | m | m | [26] 20.8 | m | m |
| 1A | Call-Info | [26] 20.9 | o | o | [26] 20.9 | o | o |
| 2 | Content-Disposition | [26] 20.11 | o | o | [26] 20.11 | m | m |
| 3 | Content-Encoding | [26] 20.12 | o | o | [26] 20.12 | m | m |
| 4 | Content-Language | [26] 20.13 | o | o | [26] 20.13 | m | m |
| 5 | Content-Length | [26] 20.14 | m | m | [26] 20.14 | m | m |
| 6 | Content-Type | [26] 20.15 | m | m | [26] 20.15 | m | m |
| 7 | Cseq | [26] 20.16 | m | m | [26] 20.16 | m | m |
| 8 | Date | [26] 20.17 | c1 | c1 | [26] 20.17 | m | m |
| 8[a] | Expires | [26] 20.19 | o | o | [26] 20.19 | o | o |
| 9 | From | [26] 20.20 | m | m | [26] 20.20 | m | m |
| 10 | MIME-Version | [26] 20.24 | o | o | [26] 20.24 | m | m |
| 11 | Organization | [26] 20.25 | o | o | [26] 20.25 | o | o |
| 11A | P-Access-Network-Info | [52] 4.4 | c5 | c6 | [52] 4.4 | c5 | c7 |
| 11B | P-Asserted-Identity | [34] 9.1 | n/a | n/a | [34] 9.1 | c3 | c3 |
| 11C | P-Charging-Function-Addresses | [52] 4.5 | c10 | c11 | [52] 4.5 | c11 | c11 |
| 11D | P-Charging-Vector | [52] 4.6 | c8 | c9 | [52] 4.6 | c8 | c9 |
| 11E | P-Preferred-Identity | [34] 9.2 | c3 | x | [34] 9.2 | n/a | n/a |
| 11F | Privacy | [33] 4.2 | c4 | c4 | [33] 4.2 | c4 | c4 |
| 11G | Reply-To | [26] 20.31 | o | o | [26] 20.31 | o | o |
| 11H | Require | [26] 20.32 | m | m | [26] 20.32 | m | m |
| 11I | Server | [26] 20.35 | o | o | [26] 20.35 | o | o |
| 12 | Timestamp | [26] 20.38 | m | m | [26] 20.38 | c2 | c2 |
| 13 | To | [26] 20.39 | m | m | [26] 20.39 | m | m |
| 13A | User-Agent | [26] 20.41 | o | o | [26] 20.41 | o | o |
| 14 | Via | [26] 20.42 | m | m | [26] 20.42 | m | m |
| 15 | Warning | [26] 20.43 | o (note) | o | [26] 20.43 | o | o |

c1: IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.
c2: IF A.4/6 THEN m ELSE n/a - - timestamping of requests.
c3: IF A.4/25 THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.
c4: IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c5: IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.
c6: IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE.
c7: IF A.4/34 AND (A.3/7A OR A.3/7D) THEN m ELSE n/a - - the P-Access-Network-Info header extension and AS acting as terminating UA or AS acting as third-party call controller.
c8: IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.
c9: IF A.4/36 THEN m ELSE n/a - - the P-Charging-Vector header extension.
c10: IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.
c11: IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.
c12: IF A.6/6 OR A.6/18 THEN m ELSE o - - 200 (OK), 405 (Method Not Allowed)

NOTE: For a 488 (Not Acceptable Here) response, RFC 3261 [26] gives the status of this header as SHOULD rather than OPTIONAL.

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/101 - - Additional for 1xx response

**Table A.50: Supported headers within the INVITE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 4 | Contact | [26] 20.10 | o | m | [26] 20.10 | m | m |
| 6 | P-Media-Authorization | [31] 5.1 | n/a | n/a | [31] 5.1 | c11 | c12 |
| 9 | Rseq | [27] 7.1 | c2 | m | [27] 7.1 | c3 | m |
| c2: | IF A.4/14 THEN o ELSE n/a - - reliability of provisional responses in SIP. | | | | | | |
| c3: | IF A.4/14 THEN m ELSE n/a - - reliability of provisional responses in SIP. | | | | | | |
| c11: | IF A.4/19 THEN m ELSE n/a - - SIP extensions for media authorization. | | | | | | |
| c12: | IF A.3/1 THEN m ELSE n/a - - UE. | | | | | | |

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/102 - - Additional for 2xx response

**Table A.51: Supported headers within the INVITE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Accept | [26] 20.1 | o | o | [26] 20.1 | m | m |
| 1A | Accept-Encoding | [26] 20.2 | o | o | [26] 20.2 | m | m |
| 1B | Accept-Language | [26] 20.3 | o | o | [26] 20.3 | m | m |
| 2 | Allow-Events | [28] 7.2.2 | c3 | c3 | [28] 7.2.2 | c4 | c4 |
| 4 | Authentication-Info | [26] 20.6 | c1 | c1 | [26] 20.6 | c2 | c2 |
| 6 | Contact | [26] 20.10 | m | m | [26] 20.10 | m | m |
| 8 | P-Media-Authorization | [31] 5.1 | n/a | n/a | [31] 5.1 | c11 | c12 |
| 9 | Record-Route | [26] 20.30 | m | m | [26] 20.30 | m | m |
| 10 | Session-Expires | [58] 4 | c13 | c13 | [58] 4 | c13 | c13 |
| 13 | Supported | [26] 20.37 | m | m | [26] 20.37 | m | m |
| c1: | IF A.4/7 THEN o ELSE n/a - - authentication between UA and UA. | | | | | | |
| c2: | IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA. | | | | | | |
| c3: | IF A.4/20 THEN o ELSE n/a - - SIP specific event notification extension. | | | | | | |
| c4: | IF A.4/20 THEN m ELSE n/a - - SIP specific event notification extension. | | | | | | |
| c11: | IF A.4/19 THEN m ELSE n/a - - SIP extensions for media authorization. | | | | | | |
| c12: | IF A.3/1 THEN m ELSE n/a - - UE. | | | | | | |
| c13: | IF A.4/42 THEN m ELSE n/a - - the SIP session timer. | | | | | | |

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/103 OR A.6/104 OR A.6/105 OR A.6/106 - - Additional for 3xx – 6xx response

**Table A.51A: Supported headers within the INVITE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Error-Info | [26] 20.18 | o | o | [26] 20.18 | o | o |

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/103 OR A.6/35 - - Additional for 3xx or 485 (Ambiguous) response

**Table A.52: Supported headers within the INVITE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 4 | Contact | [26] 20.10 | o (note 1) | o | [26] 20.10 | m | m |
| NOTE: | The strength of this requirement is RECOMMENDED rather than OPTIONAL. | | | | | | |

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/14 - - Additional for 401 (Unauthorized) response

**Table A.53: Supported headers within the INVITE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 6 | Proxy-Authenticate | [26] 20.27 | c3 | c3 | [26] 20.27 | c3 | c3 |
| 13 | WWW-Authenticate | [26] 20.44 | m | m | [26] 20.44 | m | m |
| c1: | IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses. | | | | | | |
| c2: | IF A.4/6 THEN m ELSE n/a - - timestamping of requests. | | | | | | |
| c3: | IF A.5/7 THEN m ELSE n/a - - support of authentication between UA and UA. | | | | | | |

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/17 OR A.6/23 OR A.6/30 OR A.6/36 OR A.6/50 OR A.6/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 600 (Busy Everywhere), 603 (Decline) response

**Table A.54: Supported headers within the INVITE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 8 | Retry-After | [26] 20.33 | o | o | [26] 20.33 | o | o |

**Table A.55: Void**

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/20 - - Additional for 407 (Proxy Authentication Required) response

**Table A.56: Supported headers within the INVITE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 6 | Proxy-Authenticate | [26] 20.27 | o | | [26] 20.27 | o | |
| 11 | WWW-Authenticate | [26] 20.44 | o | o | [26] 20.44 | o | o |
| c1: | IF A.5/7 THEN m ELSE n/a - - support of authentication between UA and UA. | | | | | | |

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/25 - - Additional for 415 (Unsupported Media Type) response

**Table A.57: Supported headers within the INVITE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Accept | [26] 20.1 | o.1 | o.1 | [26] 20.1 | m | m |
| 2 | Accept-Encoding | [26] 20.2 | o.1 | o.1 | [26] 20.2 | m | m |
| 3 | Accept-Language | [26] 20.3 | o.1 | o.1 | [26] 20.3 | m | m |
| o.1 | At least one of these capabilities is supported. | | | | | | |

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/27 - - Additional for 420 (Bad Extension) response

**Table A.58: Supported headers within the INVITE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 10 | Unsupported | [26] 20.40 | m | m | [26] 20.40 | m | m |

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/28 OR A.6/41A - - Additional for 421 (Extension Required), 494 (Security Agreement Required) response

**Table A.58A: Supported headers within the INVITE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 3 | Security-Server | [48] 2 | x | x | [48] 2 | c1 | c1 |
| c1: | IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. | | | | | | |

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/28A - - Additional for 422 (Session Interval Too Small) response

**Table A.58B: Supported headers within the INVITE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Min-SE | [58] 5 | c1 | c1 | [58] 5 | c1 | c1 |
| c1: | IF A.4/42 THEN o ELSE n/a - - the SIP session timer. | | | | | | |

**Table A.59: Void**

**Table A.60: Void**

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/45 - - 503 (Service Unavailable)

**Table A.61: Supported headers within the INVITE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 8 | Retry-After | [26] 20.33 | o | o | [26] 20.33 | o | m |

Prerequisite A.5/9 - - INVITE response

**Table A.62: Supported message bodies within the INVITE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | | | | | | | |

### A.2.1.4.7A MESSAGE method

Prerequisite A.5/9A - - MESSAGE request

**Table A.62A: Supported headers within the MESSAGE request**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Accept-Contact | [56B] 9.2 | c24 | c24 | [56B] 9.2 | c28 | c28 |
| 1A | Allow | [26] 20.5 | o | o | [26] 20.5 | m | m |
| 2 | Allow-Events | [28] 7.2.2 | c1 | c1 | [28] 7.2.2 | c2 | c2 |
| 3 | Authorization | [26] 20.7 | c3 | c3 | [26] 20.7 | c3 | c3 |
| 4 | Call-ID | [26] 20.8 | m | m | [26] 20.8 | m | m |
| 5 | Call-Info | [26] 20.9 | o | o | [26] 20.9 | o | o |
| 6 | Content-Disposition | [26] 20.11 | o | o | [26] 20.11 | m | m |
| 7 | Content-Encoding | [26] 20.12 | o | o | [26] 20.12 | m | m |
| 8 | Content-Language | [26] 20.13 | o | o | [26] 20.13 | m | m |
| 9 | Content-Length | [26] 20.14 | m | m | [26] 20.14 | m | m |
| 10 | Content-Type | [26] 20.15 | m | m | [26] 29.15 | m | m |
| 11 | Cseq | [26] 20.16 | m | m | [26] 20.16 | m | m |
| 12 | Date | [26] 20.17 | c4 | c4 | [26] 20.17 | m | m |
| 13 | Expires | [26] 20.19 | o | o | [26] 20.19 | o | o |
| 14 | From | [26] 20.20 | m | m | [26] 20.20 | m | m |
| 15 | In-Reply-To | [26] 20.21 | o | o | [26] 20.21 | o | o |
| 16 | Max-Forwards | [26] 20.22 | m | m | [26] 20.22 | n/a | n/a |
| 17 | MIME-Version | [26] 20.24 | o | o | [26] 20.24 | m | m |
| 18 | Organization | [26] 20.25 | o | o | [26] 20.25 | o | o |
| 18A | P-Access-Network-Info | [52] 4.4 | c15 | c16 | [52] 4.4 | c15 | c16 |
| 18B | P-Asserted-Identity | [34] 9.1 | n/a | n/a | [34] 9.1 | c11 | c11 |
| 18C | P-Called-Party-ID | [52] 4.2 | x | x | [52] 4.2 | c13 | c13 |
| 18D | P-Charging-Function-Addresses | [52] 4.5 | c20 | c21 | [52] 4.5 | c20 | c21 |
| 18E | P-Charging-Vector | [52] 4.6 | c18 | c19 | [52] 4.6 | c18 | c19 |
| 18F | P-Preferred-Identity | [34] 9.2 | c11 | c7 | [34] 9.2 | n/a | n/a |
| 18G | P-Visited-Network-ID | [52] 4.3 | x (note 1) | x | [52] 4.3 | c14 | n/a |
| 19 | Priority | [26] 20.26 | o | o | [26] 20.26 | o | o |
| 19A | Privacy | [33] 4.2 | c12 | c12 | [33] 4.2 | c12 | c12 |
| 20 | Proxy-Authorization | [26] 20.28 | c5 | c5 | [26] 20.28 | n/a | n/a |
| 21 | Proxy-Require | [26] 20.29 | o | n/a | [26] 20.29 | n/a | n/a |
| 21A | Reason | [34A] 2 | c6 | c6 | [34A] 2 | c6 | c6 |
| 22 | Record-Route | [26] 20.30 | n/a | n/a | [26] 20.30 | n/a | n/a |
| 22A | Referred-By | [59] 3 | c25 | c25 | [59] 3 | c26 | c26 |
| 23 | Reject-Contact | [56B] 9.2 | c24 | c24 | [56B] 9.2 | c28 | c28 |
| 23A | Reply-To | [26] 20.31 | o | o | [26] 20.31 | o | o |
| 23B | Request-Disposition | [56B] 9.1 | c24 | c24 | [56B] 9.1 | c28 | c28 |
| 24 | Require | [26] 20.32 | c8 | o | [26] 20.32 | m | m |
| 25 | Route | [26] 20.34 | m | m | [26] 20.34 | n/a | n/a |
| 25A | Security-Client | [48] 2.3.1 | c22 | c22 | [48] 2.3.1 | n/a | n/a |
| 25B | Security-Verify | [48] 2.3.1 | c23 | c23 | [48] 2.3.1 | n/a | n/a |
| 26 | Subject | [26] 20.35 | o | o | [26] 20.36 | o | o |
| 27 | Supported | [26] 20.37 | c9 | m | [26] 20.37 | m | m |
| 28 | Timestamp | [26] 20.38 | c10 | c10 | [26] 20.38 | m | m |
| 29 | To | [26] 20.39 | m | m | [26] 20.39 | m | m |
| 30 | User-Agent | [26] 20.41 | o | o | [26] 20.41 | o | o |
| 31 | Via | [26] 20.42 | m | m | [26] 20.42 | m | m |

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| c1: | IF A.4/20 THEN o ELSE n/a - - SIP specific event notification extension. | | | | | | |
| c2: | IF A.4/20 THEN m ELSE n/a - - SIP specific event notification extension. | | | | | | |
| c3: | IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA. | | | | | | |
| c4: | IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses. | | | | | | |
| c5: | IF A.4/8A THEN m ELSE n/a - - authentication between UA and proxy. | | | | | | |
| c6: | IF A.4/38 THEN o ELSE n/a - - the Reason header field for the session initiation protocol. | | | | | | |
| c7: | IF A.3/1 AND A.4/25 THEN o ELSE n/a - - UE and private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks. | | | | | | |
| c8: | IF A.4/14 THEN o.1 ELSE o - - Reliable transport. | | | | | | |
| c9: | IF IF A.4/14 THEN o.1 ELSE o - - support of reliable transport. | | | | | | |
| c10: | IF A.4/6 THEN o ELSE n/a - - timestamping of requests. | | | | | | |
| c11: | IF A.4/25 THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks. | | | | | | |
| c12: | IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP). | | | | | | |
| c13: | IF A.4/32 THEN o ELSE n/a - - the P-Called-Party-ID extension. | | | | | | |
| c14: | IF A.4/33 THEN o ELSE n/a - - the P-Visited-Network-ID extension. | | | | | | |
| c15: | IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension. | | | | | | |
| c16: | IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE. | | | | | | |
| c17: | IF A.4/34 AND (A.3/7A OR A.3/7D) THEN m ELSE n/a - - the P-Access-Network-Info header extension and AS acting as terminating UA or AS acting as third-party call controller. | | | | | | |
| c18: | IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension. | | | | | | |
| c19: | IF A.4/36 THEN m ELSE n/a - - the P-Charging-Vector header extension. | | | | | | |
| c20: | IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension. | | | | | | |
| c21: | IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension. | | | | | | |
| c22: | IF A.4/37 THEN o ELSE n/a - - security mechanism agreement for the session initiation protocol (note 2). | | | | | | |
| c23: | IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. | | | | | | |
| c24: | IF A.4/40 THEN o ELSE n/a - - caller preferences for the session initiation protocol. | | | | | | |
| c25: | IF A.4/43 THEN m ELSE n/a - - the SIP Referred-By mechanism. | | | | | | |
| c26: | IF A.4/43 THEN o ELSE n/a - - the SIP Referred-By mechanism. | | | | | | |
| c28: | IF A.4/40 THEN m ELSE n/a - - caller preferences for the session initiation protocol. | | | | | | |
| NOTE 1: | The strength of this requirement in RFC 3455 [52] is SHOULD NOT, rather than MUST NOT. | | | | | | |
| NOTE 2: | Support of this header in this method is dependent on the security mechanism and the security architecture which is implemented. Use of this header in this method is not appropriate to the security mechanism defined by 3GPP TS 33.203 [19]. | | | | | | |

Prerequisite A.5/9A - - MESSAGE request

**Table A.62B: Supported message bodies within the MESSAGE request**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | | | | | | | |

Prerequisite A.5/9B - - MESSAGE response for all status-codes

**Table A.62C: Supported headers within the MESSAGE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 0A | Allow | [26] 20.5 | c12 | c12 | [26] 20.5 | m | m |
| 1 | Call-ID | [26] 20.8 | m | m | [26] 20.8 | m | m |
| 2 | Call-Info | [26] 20.9 | o | o | [26] 20.9 | o | o |
| 3 | Content-Disposition | [26] 20.11 | o (note 2) | o (note 2) | [26] 20.11 | m (note 2) | m (note 2) |
| 4 | Content-Encoding | [26] 20.12 | o (note 2) | o (note 2) | [26] 20.12 | m (note 2) | m (note 2) |
| 5 | Content-Language | [26] 20.13 | o (note 2) | o (note 2) | [26] 20.13 | m (note 2) | m (note 2) |
| 6 | Content-Length | [26] 20.14 | m (note 2) | m (note 2) | [26] 20.14 | m (note 2) | m (note 2) |
| 7 | Content-Type | [26] 20.15 | m (note 2) | m (note 2) | [26] 20.15 | m (note 2) | m (note 2) |
| 8 | Cseq | [26] 20.16 | m | m | [26] 20.16 | m | m |
| 9 | Date | [26] 20.17 | c1 | c1 | [26] 20.17 | m | m |
| 9A | Expires | [26] 20.19 | o | o | [26] 20.19 | o | o |
| 10 | From | [26] 20.20 | m | m | [26] 20.20 | m | m |
| 11 | MIME-Version | [26] 20.24 | o | o | [26] 20.24 | m | m |
| 12 | Organization | [26] 20.25 | o | o | [26] 20.25 | o | o |
| 12A | P-Access-Network-Info | [52] 4.4 | c5 | c6 | [52] 4.4 | c5 | c7 |
| 12B | P-Asserted-Identity | [34] 9.1 | n/a | n/a | [34] 9.1 | c3 | c3 |
| 12C | P-Charging-Function-Addresses | [52] 4.5 | c10 | c11 | [52] 4.5 | c10 | c11 |
| 12D | P-Charging-Vector | [52] 4.6 | c8 | c9 | [52] 4.6 | c8 | c9 |
| 12E | P-Preferred-Identity | [34] 9.2 | c3 | x | [34] 9.2 | n/a | n/a |
| 12F | Privacy | [33] 4.2 | c4 | c4 | [33] 4.2 | c4 | c4 |
| 12G | Reply-To | [26] 20.31 | o | o | [26] 20.31 | o | o |
| 12H | Require | [26] 20.32 | o | o | [26] 20.32 | m | m |
| 13 | Server | [26] 20.35 | o | o | [26] 20.35 | o | o |
| 14 | Timestamp | [26] 20.38 | m | m | [26] 20.38 | c2 | c2 |
| 15 | To | [26] 20.39 | m | m | [26] 20.39 | m | m |
| 16 | User-Agent | [26] 20.41 | o | o | [26] 20.41 | o | o |
| 17 | Via | [26] 20.42 | m | m | [26] 20.42 | m | m |
| 18 | Warning | [26] 20.43 | o | o | [26] 20.43 | o | o |

c1: IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.
c2: IF A.4/6 THEN m ELSE n/a - - timestamping of requests.
c3: IF A.4/25 THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.
c4: IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c5: IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.
c6: IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE.
c7: IF A.4/34 AND (A.3/7A OR A.3/7D) THEN m ELSE n/a - - the P-Access-Network-Info header extension and AS acting as terminating UA or AS acting as third-party call controller.
c8: IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.
c9: IF A.4/36 THEN m ELSE n/a - - the P-Charging-Vector header extension.
c10: IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.
c11: IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.
c12: IF A.6/18 THEN m ELSE o - - 405 (Method Not Allowed)

NOTE 1: RFC 3261 [26] gives the status of this header as SHOULD rather than OPTIONAL.
NOTE 2: RFC 3428 [50] clause 7 states that all 2xx class responses to a MESSAGE request must not include any body, therefore for 2xx responses to the MESSAGE request the values on Sending side for "RFC status" and "Profile status" are "x", the values for Receiving side for "RFC status" and "Profile Status" are "n/a". RFC 3261 [26] subclause 7.4 states that all responses may contain bodies, therefore for all responses to the MESSAGE request other than 2xx responses, the values on Sending side for "RFC status" and "Profile status" are "o", the values for Receiving side for "RFC status" and "Profile Status" are "m".

Prerequisite A.5/9B - - MESSAGE response

Prerequisite: A.6/102 - - Additional for 2xx response

**Table A.62D: Supported headers within the MESSAGE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Allow-Events | [28] 7.2.2 | c3 | c3 | [28] 7.2.2 | c4 | c4 |
| 2 | Authentication-Info | [26] 20.6 | c1 | c1 | [26] 20.6 | c2 | c2 |
| 4 | Supported | [26] 20.37 | o | o | [26] 20.37 | m | m |
| c1: | IF A.4/7 THEN o ELSE n/a - - authentication between UA and UA. | | | | | | |
| c2: | IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA. | | | | | | |
| c3: | IF A.4/20 THEN o ELSE n/a - - SIP specific event notification extension. | | | | | | |
| c4: | IF A.4/20 THEN m ELSE n/a - - SIP specific event notification extension. | | | | | | |

Prerequisite A.5/9B - - MESSAGE response

Prerequisite: A.6/103 OR A.6/104 OR A.6/105 OR A.6/106 - - Additional for 3xx – 6xx response

**Table A.62DA: Supported headers within the MESSAGE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Error-Info | [26] 20.18 | o | o | [26] 20.18 | o | o |

Prerequisite A.5/9B - - MESSAGE response

Prerequisite: A.6/103 - - Additional for 3xx or 485 (Ambiguous) response

**Table A.62E: Supported headers within the MESSAGE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 2 | Contact | [26] 20.10 | o (note) | o | [26] 20.10 | m | m |
| NOTE: | The strength of this requirement is RECOMMENDED rather than OPTIONAL. | | | | | | |

Prerequisite A.5/9B - - MESSAGE response

Prerequisite: A.6/14 - - Additional for 401 (Unauthorized) response

**Table A.62F: Supported headers within the MESSAGE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 3 | Proxy-Authenticate | [26] 20.27 | c1 | c1 | [26] 20.27 | c1 | c1 |
| 6 | WWW-Authenticate | [26] 20.44 | m | m | [26] 20.44 | m | m |
| c1: | IF A.5/7 THEN m ELSE n/a - - support of authentication between UA and UA. | | | | | | |

Prerequisite A.5/9B - - MESSAGE response

Prerequisite: A.6/17 OR A.6/23 OR A.6/30 OR A.6/36 OR A.6/42 OR A.6/45 OR A.6/50 OR A.6/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response

**Table A.62G: Supported headers within the MESSAGE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 4 | Retry-After | [26] 20.33 | o | o | [26] 20.33 | o | o |

**Table A.62H: Void**

Prerequisite A.5/9B - - MESSAGE response

Prerequisite: A.6/20 - - Additional for 407 (Proxy Authentication Required) response

**Table A.62I: Supported headers within the MESSAGE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 3 | Proxy-Authenticate | [26] 20.27 | c1 | c1 | [26] 20.27 | c1 | c1 |
| 6 | WWW-Authenticate | [26] 20.44 | o | o | [26] 20.44 | o | o |
| c1: | IF A.5/7 THEN m ELSE n/a - - support of authentication between UA and UA. | | | | | | |

Prerequisite A.5/9B - - MESSAGE response

Prerequisite: A.6/25 - - Additional for 415 (Unsupported Media Type) response

**Table A.62J: Supported headers within the MESSAGE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Accept | [26] 20.1 | o.1 | o.1 | [26] 20.1 | m | m |
| 2 | Accept-Encoding | [26] 20.2 | o.1 | o.1 | [26] 20.2 | m | m |
| 3 | Accept-Language | [26] 20.3 | o.1 | o.1 | [26] 20.3 | m | m |
| o.1 | At least one of these capabilities is supported. | | | | | | |

Prerequisite A.5/9B - - MESSAGE response

Prerequisite: A.6/27 - - Additional for 420 (Bad Extension) response

**Table A.62K: Supported headers within the MESSAGE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 5 | Unsupported | [26] 20.40 | m | m | [26] 20.40 | m | m |

Prerequisite A.5/9B - - MESSAGE response

Prerequisite: A.6/28 OR A.6/41A - - Additional for 421 (Extension Required), 494 (Security Agreement Required) response

**Table A.62L: Supported headers within the MESSAGE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 3 | Security-Server | [48] 2 | x | x | [48] 2 | c1 | c1 |
| c1: | IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. | | | | | | |

**Table A.62M: Void**

Prerequisite A.5/9B - - MESSAGE response

**Table A.62N: Supported message bodies within the MESSAGE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | | | | | | | |

### A.2.1.4.8 NOTIFY method

Prerequisite A.5/10 - - NOTIFY request

**Table A.63: Supported headers within the NOTIFY request**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Accept | [26] 20.1 | o | o | [26] 20.1 | m | m |
| 1A | Accept-Contact | [56B] 9.2 | c19 | c19 | [56B] 9.2 | c23 | c23 |
| 2 | Accept-Encoding | [26] 20.2 | o | o | [26] 20.2 | m | m |
| 3 | Accept-Language | [26] 20.3 | o | o | [26] 20.3 | m | m |
| 3A | Allow | [26] 20.5 | o | o | [26] 20.5 | m | m |
| 4 | Allow-Events | [28] 7.2.2 | c1 | c1 | [28] 7.2.2 | c2 | c2 |
| 5 | Authorization | [26] 20.7 | c3 | c3 | [26] 20.7 | c3 | c3 |
| 6 | Call-ID | [26] 20.8 | m | m | [26] 20.8 | m | m |
| 6A | Contact | [26] 20.10 | m | m | [26] 20.10 | m | m |
| 7 | Content-Disposition | [26] 20.11 | o | o | [26] 20.11 | m | m |
| 8 | Content-Encoding | [26] 20.12 | o | o | [26] 20.12 | m | m |
| 9 | Content-Language | [26] 20.13 | o | o | [26] 20.13 | m | m |
| 10 | Content-Length | [26] 20.14 | m | m | [26] 20.14 | m | m |
| 11 | Content-Type | [26] 20.15 | m | m | [26] 20.15 | m | m |
| 12 | Cseq | [26] 20.16 | m | m | [26] 20.16 | m | m |
| 13 | Date | [26] 20.17 | c4 | c4 | [26] 20.17 | m | m |
| 14 | Event | [28] 7.2.1 | m | m | [28] 7.2.1 | m | m |
| 15 | From | [26] 20.20 | m | m | [26] 20.20 | m | m |
| 16 | Max-Forwards | [26] 20.22 | m | m | [26] 20.22 | n/a | n/a |
| 17 | MIME-Version | [26] 20.24 | o | o | [26] 20.24 | m | m |
| 17A | P-Access-Network-Info | [52] 4.4 | c10 | c11 | [52] 4.4 | c10 | c12 |
| 17B | P-Asserted-Identity | [34] 9.1 | n/a | n/a | [34] 9.1 | c6 | c6 |
| 17C | P-Charging-Function-Addresses | [52] 4.5 | c14 | c15 | [52] 4.5 | c14 | c15 |
| 17D | P-Charging-Vector | [52] 4.6 | c13 | n/a | [52] 4.6 | c13 | n/a |
| 17E | P-Preferred-Identity | [34] 9.2 | c6 | x | [34] 9.2 | n/a | n/a |
| 17F | Privacy | [33] 4.2 | c7 | n/a | [33] 4.2 | c7 | c7 |
| 18 | Proxy-Authorization | [26] 20.28 | c5 | c5 | [26] 20.28 | n/a | n/a |
| 19 | Proxy-Require | [26] 20.29 | o | n/a | [26] 20.29 | n/a | n/a |
| 19A | Reason | [34A] 2 | c18 | c18 | [34A] 2 | c18 | c18 |
| 20 | Record-Route | [26] 20.30 | n/a | n/a | [26] 20.30 | c9 | c9 |
| 20A | Referred-By | [59] 3 | c20 | c20 | [59] 3 | c21 | c21 |
| 20B | Reject-Contact | [56B] 9.2 | c19 | c19 | [56B] 9.2 | c23 | c23 |
| 20C | Request-Disposition | [56B] 9.1 | c19 | c19 | [56B] 9.1 | c23 | c23 |
| 21 | Require | [26] 20.32 | o | o | [26] 20.32 | m | m |
| 22A | Security-Client | [48] 2.3.1 | c16 | c16 | [48] 2.3.1 | n/a | n/a |
| 22B | Security-Verify | [48] 2.3.1 | c17 | c17 | [48] 2.3.1 | n/a | n/a |
| 22 | Route | [26] 20.34 | m | m | [26] 20.34 | n/a | n/a |
| 23 | Subscription-State | [28] 8.2.3 | m | m | [28] 8.2.3 | m | m |
| 24 | Supported | [26] 20.37 | o | o | [26] 20.37 | m | m |
| 25 | Timestamp | [26] 20.38 | c8 | c8 | [26] 20.38 | m | m |
| 26 | To | [26] 20.39 | m | m | [26] 20.39 | m | m |
| 27 | User-Agent | [26] 20.41 | o | o | [26] 20.41 | o | o |
| 28 | Via | [26] 20.42 | m | m | [26] 20.42 | m | m |
| 29 | Warning | [26] 20.43 | o | o | [26] 20.43 | o | o |

| | |
|---|---|
| c1: | IF A.4/20 THEN o ELSE n/a - - SIP specific event notification extension. |
| c2: | IF A.4/20 THEN m ELSE n/a - - SIP specific event notification extension. |
| c3: | IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA. |
| c4: | IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses. |
| c5: | IF A.4/8A THEN m ELSE n/a - - authentication between UA and proxy. |
| c6: | IF A.4/25 THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks. |
| c7: | IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP). |
| c8: | IF A.4/6 THEN o ELSE n/a - - timestamping of requests. |
| c9: | IF A.4/15 OR A.4/20 THEN m ELSE n/a - - the REFER method extension or SIP specific event notification extension. |
| c10: | IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension. |
| c11: | IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE. |
| c12: | IF A.4/34 AND (A.3/7A OR A.3/7D) THEN m ELSE n/a - - the P-Access-Network-Info header extension and AS acting as terminating UA or AS acting as third-party call controller. |
| c13: | IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension. |
| c14: | IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension. |
| c15: | IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension. |
| c16: | IF A.4/37 THEN o ELSE n/a - - security mechanism agreement for the session initiation protocol (note). |
| c17: | IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. |
| c18: | IF A.4/38 THEN o ELSE n/a - - the Reason header field for the session initiation protocol. |
| c19: | IF A.4/40 THEN o ELSE n/a - - caller preferences for the session initiation protocol. |
| c20: | IF A.4/43 THEN m ELSE n/a - - the SIP Referred-By mechanism. |
| c21: | IF A.4/43 THEN o ELSE n/a - - the SIP Referred-By mechanism. |
| c23: | IF A.4/40 THEN m ELSE n/a - - caller preferences for the session initiation protocol. |
| NOTE: | Support of this header in this method is dependent on the security mechanism and the security architecture which is implemented. Use of this header in this method is not appropriate to the security mechanism defined by 3GPP TS 33.203 [19]. |

Prerequisite A.5/10 - - NOTIFY request

**Table A.64: Supported message bodies within the NOTIFY request**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | sipfrag | [37] 2 | c1 | c1 | [37] | c1 | c1 |
| c1: | IF A.4/15 THEN m ELSE o - - the REFER method extension | | | | | | |

Prerequisite A.5/11 - - NOTIFY response for all status-codes

**Table A.65: Supported headers within the NOTIFY response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 0A | Allow | [26] 20.5 | o | o | [26] 20.5 | m | m |
| 1 | Call-ID | [26] 20.8 | m | m | [26] 20.8 | m | m |
| 2 | Content-Disposition | [26] 20.11 | o | o | [26] 20.11 | m | m |
| 3 | Content-Encoding | [26] 20.12 | o | o | [26] 20.12 | m | m |
| 4 | Content-Language | [26] 20.13 | o | o | [26] 20.13 | m | m |
| 5 | Content-Length | [26] 20.14 | m | m | [26] 20.14 | m | m |
| 6 | Content-Type | [26] 20.15 | m | m | [26] 20.15 | m | m |
| 7 | Cseq | [26] 20.16 | m | m | [26] 20.16 | m | m |
| 8 | Date | [26] 20.17 | c1 | c1 | [26] 20.17 | m | m |
| 9 | From | [26] 20.20 | m | m | [26] 20.20 | m | m |
| 10 | MIME-Version | [26] 20.24 | o | o | [26] 20.24 | m | m |
| 10A | P-Access-Network-Info | [52] 4.4 | c5 | c6 | [52] 4.4 | c5 | c7 |
| 10B | P-Asserted-Identity | [34] 9.1 | n/a | n/a | [34] 9.1 | c3 | c3 |
| 10C | P-Charging-Function-Addresses | [52] 4.5 | c9 | c10 | [52] 4.5 | c9 | c10 |
| 10D | P-Charging-Vector | [52] 4.6 | c8 | n/a | [52] 4.6 | c8 | n/a |
| 10E | P-Preferred-Identity | [34] 9.2 | c3 | x | [34] 9.2 | n/a | n/a |
| 10F | Privacy | [33] 4.2 | c4 | n/a | [33] 4.2 | c4 | c4 |
| 10G | Require | [26] 20.32 | m | m | [26] 20.32 | m | m |
| 10H | Server | [26] 20.35 | o | o | [26] 20.35 | o | o |
| 11 | Timestamp | [26] 20.38 | m | m | [26] 20.38 | c2 | c2 |
| 12 | To | [26] 20.39 | m | m | [26] 20.39 | m | m |
| 12A | User-Agent | [26] 20.41 | o | o | [26] 20.41 | o | o |
| 13 | Via | [26] 20.42 | m | m | [26] 20.42 | m | m |
| 14 | Warning | [26] 20.43 | o (note) | o | [26] 20.43 | o | o |
| c1: | IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses. | | | | | | |
| c2: | IF A.4/6 THEN m ELSE n/a - - timestamping of requests. | | | | | | |
| c3: | IF A.4/25 THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks. | | | | | | |
| c4: | IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP). | | | | | | |
| c5: | IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension. | | | | | | |
| c6: | IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE. | | | | | | |
| c7: | IF A.4/34 AND (A.3/7A OR A.3/7D) THEN m ELSE n/a - - the P-Access-Network-Info header extension and AS acting as terminating UA or AS acting as third-party call controller. | | | | | | |
| c8: | IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension. | | | | | | |
| c9: | IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension. | | | | | | |
| c10: | IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension. | | | | | | |
| c11: | IF A.6/18 THEN m ELSE o - - 405 (Method Not Allowed) | | | | | | |
| NOTE: | RFC 3261 [26] gives the status of this header as SHOULD rather than OPTIONAL. | | | | | | |

Prerequisite A.5/11 - - NOTIFY response

Prerequisite: A.6/102 - - Additional for 2xx response

**Table A.66: Supported headers within the NOTIFY response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 0A | Allow-Events | [28] 7.2.2 | c4 | c4 | [28] 7.2.2 | c5 | c5 |
| 1 | Authentication-Info | [26] 20.6 | c1 | c1 | [26] 20.6 | c2 | c2 |
| 1A | Contact | [26] 20.10 | o | o | [26] 20.10 | m | m |
| 2 | Record-Route | [26] 20.30 | c3 | c3 | [26] 20.30 | c3 | c3 |
| 5 | Supported | [26] 20.37 | m | m | [26] 20.37 | m | m |

| | |
|---|---|
| c1: | IF A.4/7 THEN o ELSE n/a - - authentication between UA and UA. |
| c2: | IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA. |
| c3: | IF A.4/15 OR A.4/20 THEN m ELSE n/a - - the REFER method extension or SIP specific event notification extension. |
| c4: | IF A.4/20 THEN o ELSE n/a - - SIP specific event notification extension. |
| c5: | IF A.4/20 THEN m ELSE n/a - - SIP specific event notification extension. |

Prerequisite A.5/11 - - NOTIFY response

Prerequisite: A.6/103 OR A.6/104 OR A.6/105 OR A.6/106 - - Additional for 3xx – 6xx response

**Table A.66A: Supported headers within the NOTIFY response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Error-Info | [26] 20.18 | o | o | [26] 20.18 | o | o |

Prerequisite A.5/11 - - NOTIFY response

Prerequisite: A.6/103 - - Additional for 3xx response

**Table A.67: Supported headers within the NOTIFY response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Contact | [26] 20.10 | m | m | [26] 20.10 | m | m |

Prerequisite A.5/11 - - NOTIFY response

Prerequisite: A.6/14 - - Additional for 401 (Unauthorized) response

**Table A.68: Supported headers within the NOTIFY response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 2 | Proxy-Authenticate | [26] 20.27 | c1 | c1 | [26] 20.27 | c1 | c1 |
| 8 | WWW-Authenticate | [26] 20.44 | m | m | [26] 20.44 | m | m |
| c1: | IF A.5/7 THEN m ELSE n/a - - support of authentication between UA and UA. | | | | | | |

Prerequisite A.5/11 - - NOTIFY response

Prerequisite: A.6/17 OR A.6/23 OR A.6/30 OR A.6/36 OR A.6/42 OR A.6/45 OR A.6/50 OR A.6/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response

**Table A.69: Supported headers within the NOTIFY response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 3 | Retry-After | [26] 20.33 | o | o | [26] 20.33 | o | o |

**Table A.70: Void**

Prerequisite A.5/11 - - NOTIFY response

Prerequisite: A.6/20 - - Additional for 407 (Proxy Authentication Required) response

**Table A.71: Supported headers within the NOTIFY response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 2 | Proxy-Authenticate | [26] 20.27 | c3 | c3 | [26] 20.27 | c3 | c3 |
| 6 | WWW-Authenticate | [26] 20.44 | o | o | [26] 20.44 | o | o |
| c3: | IF A.5/7 THEN m ELSE n/a - - support of authentication between UA and UA. | | | | | | |

Prerequisite A.5/11 - - NOTIFY response

Prerequisite A.6/25 - - Additional for 415 (Unsupported Media Type) response

**Table A.72: Supported headers within the NOTIFY response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Accept | [26] 20.1 | o.1 | o.1 | [26] 20.1 | m | m |
| 2 | Accept-Encoding | [26] 20.2 | o.1 | o.1 | [26] 20.2 | m | m |
| 3 | Accept-Language | [26] 20.3 | o.1 | o.1 | [26] 20.3 | m | m |
| o.1 | At least one of these capabilities is supported. | | | | | | |

Prerequisite A.5/11 - - NOTIFY response

Prerequisite: A.6/27 - - Addition for 420 (Bad Extension) response

**Table A.73: Supported headers within the NOTIFY response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 5 | Unsupported | [26] 20.40 | m | m | [26] 20.40 | m | m |

Prerequisite A.5/11 - - NOTIFY response

Prerequisite: A.6/28 OR A.6/41A - - Additional for 421 (Extension Required), 494 (Security Agreement Required) response

**Table A.73A: Supported headers within the NOTIFY response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 3 | Security-Server | [48] 2 | x | x | [48] 2 | c1 | c1 |
| c1: | IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. | | | | | | |

**Table A.74: Void**

Prerequisite A.5/11 - - NOTIFY response

Prerequisite: A.6/35 - - Additional for 485 (Ambigious) response

**Table A.74A: Supported headers within the NOTIFY response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Contact | [26] 20.10 | o | o | [26] 20.10 | m | m |

Prerequisite A.5/11 - - NOTIFY response

Prerequisite: A.6/39 - - Additional for 489 (Bad Event) response

**Table A.75: Supported headers within the NOTIFY response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Allow-Events | [28] 7.2.2 | m | m | [28] 7.2.2 | m | m |

Prerequisite A.5/11 - - NOTIFY response

**Table A.76: Supported message bodies within the NOTIFY response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | | | | | | | |

### A.2.1.4.9 OPTIONS method

Prerequisite A.5/12 - - OPTIONS request

**Table A.77: Supported headers within the OPTIONS request**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Accept | [26] 20.1 | m | m | [26] 20.1 | m | m |
| 1A | Accept-Contact | [56B] 9.2 | c21 | c21 | [56B] 9.2 | c26 | c26 |
| 2 | Accept-Encoding | [26] 20.2 | m | m | [26] 20.2 | m | m |
| 3 | Accept-Language | [26] 20.3 | m | m | [26] 20.3 | m | m |
| 3A | Allow | [26] 20.5 | o | o | [26] 20.5 | m | m |
| 4 | Allow-Events | [28] 7.2.2 | c24 | c24 | [28] 7.2.2 | c1 | c1 |
| 5 | Authorization | [26] 20.7 | c2 | c2 | [26] 20.7 | c2 | c2 |
| 6 | Call-ID | [26] 20.8 | m | m | [26] 20.8 | m | m |
| 7 | Call-Info | [26] 20.9 | o | o | [26] 20.9 | o | o |
| 8 | Contact | [26] 20.10 | o | o | [26] 20.10 | o | o |
| 9 | Content-Disposition | [26] 20.11 | o | o | [26] 20.11 | m | m |
| 10 | Content-Encoding | [26] 20.12 | o | o | [26] 20.12 | m | m |
| 11 | Content-Language | [26] 20.13 | o | o | [26] 20.13 | m | m |
| 12 | Content-Length | [26] 20.14 | m | m | [26] 20.14 | m | m |
| 13 | Content-Type | [26] 20.15 | m | m | [26] 20.15 | m | m |
| 14 | Cseq | [26] 20.16 | m | m | [26] 20.16 | m | m |
| 15 | Date | [26] 20.17 | c3 | c3 | [26] 20.17 | m | m |
| 16 | From | [26] 20.20 | m | m | [26] 20.20 | m | m |
| 17 | Max-Forwards | [26] 20.22 | m | m | [26] 20.22 | n/a | n/a |
| 18 | MIME-Version | [26] 20.24 | o | o | [26] 20.24 | m | m |
| 19 | Organization | [26] 20.25 | o | o | [26] 20.25 | o | o |
| 19A | P-Access-Network-Info | [52] 4.4 | c11 | c12 | [52] 4.4 | c11 | c13 |
| 19B | P-Asserted-Identity | [34] 9.1 | n/a | n/a | [34] 9.1 | c6 | c6 |
| 19C | P-Called-Party-ID | [52] 4.2 | x | x | [52] 4.2 | c9 | c9 |
| 19D | P-Charging-Function-Addresses | [52] 4.5 | c16 | c17 | [52] 4.5 | c16 | c17 |
| 19E | P-Charging-Vector | [52] 4.6 | c14 | c15 | [52] 4.6 | c14 | c15 |
| 19F | P-Preferred-Identity | [34] 9.2 | c6 | c4 | [34] 9.2 | n/a | n/a |
| 19G | P-Visited-Network-ID | [52] 4.3 | x (note 2) | x | [52] 4.3 | c10 | n/a |
| 19H | Privacy | [33] 4.2 | c8 | c8 | [33] 4.2 | c8 | c8 |
| 20 | Proxy-Authorization | [26] 20.28 | c5 | c5 | [26] 20.28 | n/a | n/a |
| 21 | Proxy-Require | [26] 20.29 | o | o (note 1) | [26] 20.29 | n/a | n/a |
| 21A | Reason | [34A] 2 | c20 | c20 | [34A] 2 | c20 | c20 |
| 22 | Record-Route | [26] 20.30 | n/a | n/a | [26] 20.30 | n/a | n/a |
| 22A | Referred-By | [59] 3 | c22 | c22 | [59] 3 | c23 | c23 |
| 22B | Reject-Contact | [56B] 9.2 | c21 | c21 | [56B] 9.2 | c26 | c26 |
| 22C | Request-Disposition | [56B] 9.1 | c21 | c21 | [56B] 9.1 | c26 | c26 |
| 23 | Require | [26] 20.32 | o | o | [26] 20.32 | m | m |
| 24 | Route | [26] 20.34 | m | m | [26] 20.34 | n/a | n/a |
| 24A | Security-Client | [48] 2.3.1 | c18 | c18 | [48] 2.3.1 | n/a | n/a |
| 24B | Security-Verify | [48] 2.3.1 | c19 | c19 | [48] 2.3.1 | n/a | n/a |
| 25 | Supported | [26] 20.37 | c6 | c6 | [26] 20.37 | m | m |
| 26 | Timestamp | [26] 20.38 | c7 | c7 | [26] 20.38 | m | m |
| 27 | To | [26] 20.39 | m | m | [26] 20.39 | m | m |
| 28 | User-Agent | [26] 20.41 | o | o | [26] 20.41 | o | o |
| 29 | Via | [26] 20.42 | m | m | [26] 20.42 | m | m |

| | |
|---|---|
| c1: | IF A.4/20 THEN m ELSE n/a - - SIP specific event notification extension. |
| c2: | IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA. |
| c3: | IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses. |
| c4: | IF A.3/1 AND A.4/25 THEN o ELSE n/a - - UE and private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks. |
| c5: | IF A.4/8A THEN m ELSE n/a - - authentication between UA and proxy. |
| c6: | IF A.4/25 THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks. |
| c7: | IF A.4/6 THEN o ELSE n/a - - timestamping of requests. |
| c8: | IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP). |
| c9: | IF A.4/32 THEN o ELSE n/a - - the P-Called-Party-ID extension. |
| c10: | IF A.4/33 THEN o ELSE n/a - - the P-Visited-Network-ID extension. |
| c11: | IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension. |
| c12: | IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE. |
| c13: | IF A.4/34 AND (A.3/7A OR A.3/7D) THEN m ELSE n/a - - the P-Access-Network-Info header extension and AS acting as terminating UA or AS acting as third-party call controller. |
| c14: | IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension. |
| c15: | IF A.4/36 THEN m ELSE n/a - - the P-Charging-Vector header extension. |
| c16: | IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension. |
| c17: | IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension. |
| c18: | IF A.4/37 THEN o ELSE n/a - - security mechanism agreement for the session initiation protocol (note 3). |
| c19: | IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. |
| c20: | IF A.4/38 THEN o ELSE n/a - - the Reason header field for the session initiation protocol. |
| c21: | IF A.4/40 THEN o ELSE n/a - - caller preferences for the session initiation protocol. |
| c22: | IF A.4/43 THEN m ELSE n/a - - the SIP Referred-By mechanism. |
| c23: | IF A.4/43 THEN o ELSE n/a - - the SIP Referred-By mechanism. |
| c24: | IF A.4/20 THEN o ELSE n/a - - SIP specific event notification extension. |
| c26: | IF A.4/40 THEN m ELSE n/a - - caller preferences for the session initiation protocol. |
| NOTE 1: | No distinction has been made in these tables between first use of a request on a From/To/Call-ID combination, and the usage in a subsequent one. Therefore the use of "o" etc. above has been included from a viewpoint of first usage. |
| NOTE 2: | The strength of this requirement in RFC 3455 [52] is SHOULD NOT, rather than MUST NOT. |
| NOTE 3: | Support of this header in this method is dependent on the security mechanism and the security architecture which is implemented. Use of this header in this method is not appropriate to the security mechanism defined by 3GPP TS 33.203 [19]. |

Prerequisite A.5/12 - - OPTIONS request

**Table A.78: Supported message bodies within the OPTIONS request**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | | | | | | | |

**Table A.79: Void**

Prerequisite A.5/13 - - OPTIONS response for all status-codes

**Table A.80: Supported headers within the OPTIONS response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 0A | Allow | [26] 20.5 | c12 | c12 | [26] 20.5 | m | m |
| 1 | Call-ID | [26] 20.8 | m | m | [26] 20.8 | m | m |
| 1A | Call-Info | [26] 20.9 | o | o | [26] 20.9 | o | o |
| 2 | Content-Disposition | [26] 20.11 | o | o | [26] 20.11 | m | m |
| 3 | Content-Encoding | [26] 20.12 | o | o | [26] 20.12 | m | m |
| 4 | Content-Language | [26] 20.13 | o | o | [26] 20.13 | m | m |
| 5 | Content-Length | [26] 20.14 | m | m | [26] 20.14 | m | m |
| 6 | Content-Type | [26] 20.15 | m | m | [26] 20.15 | m | m |
| 7 | Cseq | [26] 20.16 | m | m | [26] 20.16 | m | m |
| 8 | Date | [26] 20.17 | c1 | c1 | [26] 20.17 | m | m |
| 9 | From | [26] 20.20 | m | m | [26] 20.20 | m | m |
| 10 | MIME-Version | [26] 20.24 | o | o | [26] 20.24 | m | m |
| 11 | Organization | [26] 20.25 | o | o | [26] 20.25 | o | o |
| 11A | P-Access-Network-Info | [52] 4.4 | c5 | c6 | [52] 4.4 | c5 | c7 |
| 11B | P-Asserted-Identity | [34] 9.1 | n/a | n/a | [34] 9.1 | c3 | c3 |
| 11C | P-Charging-Function-Addresses | [52] 4.5 | c10 | c11 | [52] 4.5 | c10 | c11 |
| 11D | P-Charging-Vector | [52] 4.6 | c8 | c9 | [52] 4.6 | c8 | c9 |
| 11E | P-Preferred-Identity | [34] 9.2 | c3 | x | [34] 9.2 | n/a | n/a |
| 11F | Privacy | [33] 4.2 | c4 | c4 | [33] 4.2 | c4 | c4 |
| 11G | Require | [26] 20.32 | m | m | [26] 20.32 | m | m |
| 11H | Server | [26] 20.35 | o | o | [26] 20.35 | o | o |
| 12 | Timestamp | [26] 20.38 | m | m | [26] 20.38 | c2 | c2 |
| 13 | To | [26] 20.39 | m | m | [26] 20.39 | m | m |
| 13A | User-Agent | [26] 20.41 | o | o | [26] 20.41 | o | o |
| 14 | Via | [26] 20.42 | m | m | [26] 20.42 | m | m |
| 15 | Warning | [26] 20.43 | o (note) | o | [26] 20.43 | o | o |
| c1: | IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses. | | | | | | |
| c2: | IF A.4/6 THEN m ELSE n/a - - timestamping of requests. | | | | | | |
| c3: | IF A.4/25 THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks. | | | | | | |
| c4: | IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP). | | | | | | |
| c5: | IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension. | | | | | | |
| c6: | IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE. | | | | | | |
| c7: | IF A.4/34 AND (A.3/7A OR A.3/7D) THEN m ELSE n/a - - the P-Access-Network-Info header extension and AS acting as terminating UA or AS acting as third-party call controller. | | | | | | |
| c8: | IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension. | | | | | | |
| c9: | IF A.4/36 THEN m ELSE n/a - - the P-Charging-Vector header extension. | | | | | | |
| c10: | IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension. | | | | | | |
| c11: | IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension. | | | | | | |
| c12: | IF A.6/6 OR A.6/18 THEN m ELSE o - - 200 (OK), 405 (Method Not Allowed) | | | | | | |
| NOTE: | RFC 3261 [26] gives the status of this header as SHOULD rather than OPTIONAL. | | | | | | |

Prerequisite A.5/13 - - OPTIONS response

Prerequisite: A.6/102 - - Additional for 2xx response

**Table A.81: Supported headers within the OPTIONS response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Accept | [26] 20.1 | m | m | [26] 20.1 | m | m |
| 1A | Accept-Encoding | [26] 20.2 | m | m | [26] 20.2 | m | m |
| 1B | Accept-Language | [26] 20.3 | m | m | [26] 20.3 | m | m |
| 2 | Allow-Events | [28] 7.2.2 | c3 | c3 | [28] 7.2.2 | c4 | c4 |
| 3 | Authentication-Info | [26] 20.6 | c1 | c1 | [26] 20.6 | c2 | c2 |
| 5 | Contact | [26] 20.10 | o | | [26] 20.10 | o | |
| 8 | Supported | [26] 20.37 | m | m | [26] 20.37 | m | m |
| c1: | IF A.4/7 THEN o ELSE n/a - - authentication between UA and UA. | | | | | | |
| c2: | IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA. | | | | | | |
| c3: | IF A.4/20 THEN o ELSE n/a - - SIP specific event notification extension. | | | | | | |
| c4: | IF A.4/20 THEN m ELSE n/a - - SIP specific event notification extension. | | | | | | |

Prerequisite A.5/13 - - OPTIONS response

Prerequisite: A.6/103 OR A.6/104 OR A.6/105 OR A.6/106 - - Additional for 3xx – 6xx response

**Table A.81A: Supported headers within the OPTIONS response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Error-Info | [26] 20.18 | o | o | [26] 20.18 | o | o |

Prerequisite A.5/13 - - OPTIONS response

Prerequisite: A.6/103 OR A.6/35 - - Additional for 3xx or 485 (Ambiguous) response

**Table A.82: Supported headers within the OPTIONS response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 3 | Contact | [26] 20.10 | o (note) | o | [26] 20.10 | m | m |
| NOTE: | RFC 3261 [26] gives the status of this header as SHOULD rather than OPTIONAL. | | | | | | |

Prerequisite A.5/13 - - OPTIONS response

Prerequisite: A.6/14 - - Additional for 401 (Unauthorized) response

**Table A.83: Supported headers within the OPTIONS response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 4 | Proxy-Authenticate | [26] 20.27 | c1 | c1 | [26] 20.27 | c1 | c1 |
| 10 | WWW-Authenticate | [26] 20.44 | o | | [26] 20.44 | o | |
| c1: | IF A.5/7 THEN m ELSE n/a - - support of authentication between UA and UA. | | | | | | |

Prerequisite A.5/13 - - OPTIONS response

Prerequisite: A.6/17 OR A.6/23 OR A.6/30 OR A.6/36 OR A.6/42 OR A.6/45 OR A.6/50 OR A.6/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response.

**Table A.84: Supported headers within the OPTIONS response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 5 | Retry-After | [26] 20.33 | o | o | [26] 20.33 | o | o |

**Table A.85: Void**

Prerequisite A.5/13 - - OPTIONS response

Prerequisite: A.6/20 - - Additional for 407 (Proxy Authentication Required) response

**Table A.86: Supported headers within the OPTIONS response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 4 | Proxy-Authenticate | [26] 20.27 | c1 | c1 | [26] 20.27 | c1 | c1 |
| 8 | WWW-Authenticate | [26] 20.44 | o | o | [26] 20.44 | o | o |
| c1: | IF A.5/7 THEN m ELSE n/a - - support of authentication between UA and UA. | | | | | | |

Prerequisite A.5/13 - - OPTIONS response

Prerequisite: A.6/25 - - Additional for 415 (Unsupported Media Type) response

**Table A.87: Supported headers within the OPTIONS response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Accept | [26] 20.1 | o.1 | o.1 | [26] 20.1 | m | m |
| 2 | Accept-Encoding | [26] 20.2 | o.1 | o.1 | [26] 20.2 | m | m |
| 3 | Accept-Language | [26] 20.3 | o.1 | o.1 | [26] 20.3 | m | m |
| o.1 | At least one of these capabilities is supported. | | | | | | |

Prerequisite A.5/13 - - OPTIONS response

Prerequisite: A.6/27 - - Additional for 420 (Bad Extension) response

**Table A.88: Supported headers within the OPTIONS response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 7 | Unsupported | [26] 20.40 | m | m | [26] 20.40 | m | m |

Prerequisite A.5/13 - - OPTIONS response

Prerequisite: A.6/28 OR A.6/41A - - Additional 421 (Extension Required), 494 (Security Agreement Required) response

**Table A.88A: Supported headers within the OPTIONS response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 3 | Security-Server | [48] 2 | x | x | [48] 2 | c1 | c1 |
| c1: | IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. | | | | | | |

**Table A.89: Void**

Prerequisite A.5/13 - - OPTIONS response

**Table A.90: Supported message bodies within the OPTIONS response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | | | | | | | |

### A.2.1.4.10 PRACK method

Prerequisite A.5/14 - - PRACK request

**Table A.91: Supported headers within the PRACK request**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Accept | [26] 20.1 | o | o | [26] 20.1 | m | m |
| 1A | Accept-Contact | [56B] 9.2 | c15 | c15 | [56B] 9.2 | c18 | c18 |
| 2 | Accept-Encoding | [26] 20.2 | o | o | [26] 20.2 | m | m |
| 3 | Accept-Language | [26] 20.3 | o | o | [26] 20.3 | m | m |
| 3A | Allow | [26] 20.5 | o | o | [26] 20.5 | m | m |
| 4 | Allow-Events | [28] 7.2.2 | c1 | c1 | [28] 7.2.2 | c2 | c2 |
| 5 | Authorization | [26] 20.7 | c3 | c3 | [26] 20.7 | c3 | c3 |
| 6 | Call-ID | [26] 20.8 | m | m | [26] 20.8 | m | m |
| 7 | Content-Disposition | [26] 20.11 | o | o | [26] 20.11 | m | m |
| 8 | Content-Encoding | [26] 20.12 | o | o | [26] 20.12 | m | m |
| 9 | Content-Language | [26] 20.13 | o | o | [26] 20.13 | m | m |
| 10 | Content-Length | [26] 20.14 | m | m | [26] 20.14 | m | m |
| 11 | Content-Type | [26] 20.15 | m | m | [26] 20.15 | m | m |
| 12 | Cseq | [26] 20.16 | m | m | [26] 20.16 | m | m |
| 13 | Date | [26] 20.17 | c4 | c4 | [26] 20.17 | m | m |
| 14 | From | [26] 20.20 | m | m | [26] 20.20 | m | m |
| 15 | Max-Forwards | [26] 20.22 | m | m | [26] 20.22 | n/a | n/a |
| 16 | MIME-Version | [26] 20.24 | o | o | [26] 20.24 | m | m |
| 16A | P-Access-Network-Info | [52] 4.4 | c9 | c10 | [52] 4.4 | c9 | c11 |
| 16B | P-Charging-Function-Addresses | [52] 4.5 | c13 | c14 | [52] 4.5 | c13 | c14 |
| 16C | P-Charging-Vector | [52] 4.6 | c12 | n/a | [52] 4.6 | c12 | n/a |
| 16D | Privacy | [33] 4.2 | c6 | n/a | [33] 4.2 | c6 | n/a |
| 17 | Proxy-Authorization | [26] 20.28 | c5 | c5 | [26] 20.28 | n/a | n/a |
| 18 | Proxy-Require | [26] 20.29 | o | n/a | [26] 20.29 | n/a | n/a |
| 19 | Rack | [27] 7.2 | m | m | [27] 7.2 | m | m |
| 19A | Reason | [34A] 2 | c7 | c7 | [34A] 2 | c7 | c7 |
| 20 | Record-Route | [26] 20.30 | n/a | n/a | [26] 20.30 | n/a | n/a |
| 20A | Referred-By | [59] 3 | c16 | c16 | [59] 3 | c17 | c17 |
| 20B | Reject-Contact | [56B] 9.2 | c15 | c15 | [56B] 9.2 | c18 | c18 |
| 20C | Request-Disposition | [56B] 9.1 | c15 | c15 | [56B] 9.1 | c18 | c18 |
| 21 | Require | [26] 20.32 | o | o | [26] 20.32 | m | m |
| 22 | Route | [26] 20.34 | m | m | [26] 20.34 | n/a | n/a |
| 23 | Supported | [26] 20.37 | o | o | [26] 20.37 | m | m |
| 24 | Timestamp | [26] 20.38 | c8 | c8 | [26] 20.38 | m | m |
| 25 | To | [26] 20.39 | m | m | [26] 20.39 | m | m |
| 26 | User-Agent | [26] 20.41 | o | o | [26] 20.41 | o | o |
| 27 | Via | [26] 20.42 | m | m | [26] 20.42 | m | m |

c1: IF A.4/20 THEN o ELSE n/a - - SIP specific event notification extension.
c2: IF A.4/20 THEN m ELSE n/a - - SIP specific event notification extension.
c3: IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA.
c4: IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.
c5: IF A.4/8A THEN m ELSE n/a - - authentication between UA and proxy.
c6: IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c7: IF A.4/38 THEN o ELSE n/a - - the Reason header field for the session initiation protocol.
c8: IF A.4/6 THEN o ELSE n/a - - timestamping of requests.
c9: IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.
c10: IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE.
c11: IF A.4/34 AND (A.3/7A OR A.3/7D) THEN m ELSE n/a - - the P-Access-Network-Info header extension and AS acting as terminating UA or AS acting as third-party call controller.
c12: IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.
c13: IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.
c14: IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.
c15: IF A.4/40 THEN o ELSE n/a - - caller preferences for the session initiation protocol.
c16: IF A.4/43 THEN m ELSE n/a - - the SIP Referred-By mechanism.
c17: IF A.4/43 THEN o ELSE n/a - - the SIP Referred-By mechanism.
c18: IF A.4/40 THEN m ELSE n/a - - caller preferences for the session initiation protocol.

Prerequisite A.5/14 - - PRACK request

**Table A.92: Supported message bodies within the PRACK request**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | | | | | | | |

**Table A.93: Void**

Prerequisite A.5/15 - - PRACK response for all status-codes

**Table A.94: Supported headers within the PRACK response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 0A | Allow | [26] 20.5 | c9 | c9 | [26] 20.5 | m | m |
| 1 | Call-ID | [26] 20.8 | m | m | [26] 20.8 | m | m |
| 2 | Content-Disposition | [26] 20.11 | o | o | [26] 20.11 | m | m |
| 3 | Content-Encoding | [26] 20.12 | o | o | [26] 20.12 | m | m |
| 4 | Content-Language | [26] 20.13 | o | o | [26] 20.13 | m | m |
| 5 | Content-Length | [26] 20.14 | m | m | [26] 20.14 | m | m |
| 6 | Content-Type | [26] 20.15 | m | m | [26] 20.15 | m | m |
| 7 | Cseq | [26] 20.16 | m | m | [26] 20.16 | m | m |
| 8 | Date | [26] 20.17 | c1 | c1 | [26] 20.17 | m | m |
| 9 | From | [26] 20.20 | m | m | [26] 20.20 | m | m |
| 10 | MIME-Version | [26] 20.24 | o | o | [26] 20.24 | m | m |
| 10A | P-Access-Network-Info | [52] 4.4 | c3 | c4 | [52] 4.4 | c3 | c5 |
| 10B | P-Charging-Function-Addresses | [52] 4.5 | c7 | c8 | [52] 4.5 | c7 | c8 |
| 10C | P-Charging-Vector | [52] 4.6 | c6 | n/a | [52] 4.6 | c6 | n/a |
| 10D | Privacy | [33] 4.2 | c2 | n/a | [33] 4.2 | c2 | n/a |
| 10E | Require | [26] 20.32 | o | o | [26] 20.32 | m | m |
| 10F | Server | [26] 20.35 | o | o | [26] 20.35 | o | o |
| 11 | Timestamp | [26] 20.38 | m | m | [26] 20.38 | c2 | c2 |
| 12 | To | [26] 20.39 | m | m | [26] 20.39 | m | m |
| 12A | User-Agent | [26] 20.41 | o | o | [26] 20.41 | o | o |
| 13 | Via | [26] 20.42 | m | m | [26] 20.42 | m | m |
| 14 | Warning | [26] 20.43 | o (note) | o | [26] 20.43 | o | o |
| c1: | IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses. | | | | | | |
| c2: | IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP). | | | | | | |
| c3: | IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension. | | | | | | |
| c4: | IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE. | | | | | | |
| c5: | IF A.4/34 AND (A.3/7A OR A.3/7D) THEN m ELSE n/a - - the P-Access-Network-Info header extension and AS acting as terminating UA or AS acting as third-party call controller. | | | | | | |
| c6: | IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension. | | | | | | |
| c7: | IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension. | | | | | | |
| c8: | IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension. | | | | | | |
| c9: | IF A.6/18 THEN m ELSE o - - 405 (Method Not Allowed) | | | | | | |
| NOTE: | RFC 3261 [26] gives the status of this header as SHOULD rather than OPTIONAL. | | | | | | |

Prerequisite A.5/15 - - PRACK response

Prerequisite: A.6/102 - - Additional for 2xx response

**Table A.95: Supported headers within the PRACK response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 0A | Allow-Events | [28] 7.2.2 | c3 | c3 | [28] 7.2.2 | c4 | c4 |
| 0B | Authentication-Info | [26] 20.6 | c1 | c1 | [26] 20.6 | c2 | c2 |
| 3 | Supported | [26] 20.37 | m | m | [26] 20.37 | m | m |
| c1: | IF A.4/7 THEN o ELSE n/a - - authentication between UA and UA. | | | | | | |
| c2: | IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA. | | | | | | |
| c3: | IF A.4/20 THEN o ELSE n/a - - SIP specific event notification extension. | | | | | | |
| c4: | IF A.4/20 THEN m ELSE n/a - - SIP specific event notification extension. | | | | | | |

Prerequisite A.5/15 - - PRACK response

Prerequisite: A.6/103 OR A.6/104 OR A.6/105 OR A.6/106 - - Additional for 3xx – 6xx response

**Table A.95A: Supported headers within the PRACK response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Error-Info | [26] 20.18 | o | o | [26] 20.18 | o | o |

Prerequisite A.5/15 - - PRACK response

Prerequisite: A.6/103 OR A.6/35 - - Additional for 3xx or 485 (Ambiguous) response

**Table A.96: Supported headers within the PRACK response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Contact | [26] 20.10 | o (note) | o | [26] 20.10 | m | m |
| NOTE: | RFC 3261 [26] gives the status of this header as SHOULD rather than OPTIONAL. | | | | | | |

Prerequisite A.5/15 - - PRACK response

Prerequisite: A.6/14 - - Additional for 401 (Unauthorized) response

**Table A.97: Supported headers within the PRACK response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 2 | Proxy-Authenticate | [26] 20.27 | c1 | c1 | [26] 20.27 | c1 | c1 |
| 8 | WWW-Authenticate | [26] 20.44 | m | m | [26] 20.44 | m | m |
| c1: | IF A.5/7 THEN m ELSE n/a - - support of authentication between UA and UA. | | | | | | |

Prerequisite A.5/15 - - PRACK response

Prerequisite: A.6/17 OR A.6/23 OR A.6/30 OR A.6/36 OR A.6/42 OR A.6/45 OR A.6/50 OR A.6/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response.

**Table A.98: Supported headers within the PRACK response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 3 | Retry-After | [26] 20.33 | o | o | [26] 20.33 | o | o |

**Table A.99: Void**

Prerequisite A.5/15 - - PRACK response

Prerequisite: A.6/20 - - Additional for 407 (Proxy Authentication Required) response

**Table A.100: Supported headers within the PRACK response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 2 | Proxy-Authenticate | [26] 20.27 | c1 | c1 | [26] 20.27 | c1 | c1 |
| 6 | WWW-Authenticate | [26] 20.44 | o | o | [26] 20.44 | o | o |
| c1: | IF A.5/7 THEN m ELSE n/a - - support of authentication between UA and UA. | | | | | | |

Prerequisite A.5/15 - - PRACK response

Prerequisite: A.6/25 - - Additional for 415 (Unsupported Media Type) response

**Table A.101: Supported headers within the PRACK response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Accept | [26] 20.1 | o.1 | o.1 | [26] 20.1 | m | m |
| 2 | Accept-Encoding | [26] 20.2 | o.1 | o.1 | [26] 20.2 | m | m |
| 3 | Accept-Language | [26] 20.3 | o.1 | o.1 | [26] 20.3 | m | m |

Prerequisite A.5/15 - - PRACK response

Prerequisite: A.6/27 - - Additional for 420 (Bad Extension) response

**Table A.102: Supported headers within the PRACK response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 5 | Unsupported | [26] 20.40 | m | m | [26] 20.40 | m | m |

Prerequisite A.5/15 - - PRACK response

Prerequisite: A.6/28 OR A.6/41A - - Additional for 421 (Extension Required), 494 (Security Agreement Required) response

**Table A.102A: Supported headers within the PRACK response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 3 | Security-Server | [48] 2 | x | x | [48] 2 | c1 | c1 |
| c1: | IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. | | | | | | |

**Table A.103: Void**

Prerequisite A.5/15 - - PRACK response

**Table A.104: Supported message bodies within the PRACK response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | | | | | | | |

### A.2.1.4.10A PUBLISH method

Prerequisite A.5/15A – PUBLISH request

**Table A.104A: Supported headers within the PUBLISH request**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Accept-Contact | [56B] 9.2 | c22 | c22 | [56B] 9.2 | c28 | c28 |
| 2 | Allow | [26] 20.5 | o | o | [26] 20.5 | m | m |
| 3 | Allow-Events | [26] 7.2.2 | c1 | c1 | [26] 7.2.2 | c2 | c2 |
| 4 | Authorization | [26] 20.7 | c3 | c3 | [26] 20.7 | c3 | c3 |
| 5 | Call-ID | [26] 20.8 | m | m | [26] 20.8 | m | m |
| 6 | Call-Info | [26] 20.9 | o | o | [26] 20.9 | o | o |
| 7 | Content-Disposition | [26] 20.11 | o | o | [26] 20.11 | m | m |
| 8 | Content-Encoding | [26] 20.12 | o | o | [26] 20.12 | m | m |
| 9 | Content-Language | [26] 20.13 | o | o | [26] 20.13 | m | m |
| 10 | Content-Length | [26] 20.14 | m | m | [26] 20.14 | m | m |
| 11 | Content-Type | [26] 20.15 | m | m | [26] 20.15 | m | m |
| 12 | Cseq | [26] 20.16 | m | m | [26] 20.16 | m | m |
| 13 | Date | [26] 20.17 | c4 | c4 | [26] 20.17 | m | m |
| 14 | Event | [70] 4, 6 | m | m | [70] 4, 6 | m | m |
| 15 | Expires | [26] 20.19, [70] 4, 5, 6 | o | o | [26] 20.19, [70] 4, 5, 6 | m | m |
| 16 | From | [26] 20.20 | m | m | [26] 20.20 | m | m |
| 17 | In-Reply-To | [26] 20.21 | o | o | [26] 20.21 | o | o |
| 18 | Max-Forwards | [26] 20.22 | m | m | [26] 20.22 | n/a | n/a |
| 19 | MIME-Version | [26] 20.24 | o | o | [26] 20.24 | m | m |
| 20 | Organization | [26] 20.25 | o | o | [26] 20.25 | o | o |
| 21 | P-Access-Network-Info | [52] 4.4 | c15 | c16 | [52] 4.4 | c15 | c17 |
| 22 | P-Asserted-Identity | [34] 9.1 | n/a | n/a | [34] 9.1 | c11 | c11 |
| 23 | P-Called-Party-ID | [52] 4.2 | x | x | [52] 4.2 | c13 | c13 |
| 24 | P-Charging-Function-Addresses | [52] 4.5 | c20 | c21 | [52] 4.5 | c20 | c21 |
| 25 | P-Charging-Vector | [52] 4.6 | c18 | c19 | [52] 4.6 | c18 | c19 |
| 26 | P-Preferred-Identity | [34] 9.2 | c11 | c7 | [34] 9.2 | n/a | n/a |
| 27 | P-Visited-Network-ID | [52] 4.3 | x (note 3) | x | [52] 4.3 | c14 | n/a |
| 28 | Priorità | [26] 20.26 | o | o | [26] 20.26 | o | o |
| 29 | Privacy | [33] 4.2 | c12 | c12 | [33] 4.2 | c12 | c12 |
| 30 | Proxy-Authorization | [26] 20.28 | c5 | c5 | [26] 20.28 | n/a | n/a |
| 31 | Proxy-Require | [26] 20.29 | o | n/a | [26] 20.29 | n/a | n/a |
| 32 | Reason | [34A] 2 | c8 | c8 | [34A] 2 | c8 | c8 |
| 33 | Reject-Contact | [56B] 9.2 | c22 | c22 | [56B] 9.2 | c28 | c28 |
| 33A | Referred-By | [59] 3 | c25 | c25 | [59] 3 | c26 | c26 |
| 34 | Request-Disposition | [56B] 9.1 | c22 | c22 | [56B] 9.1 | c28 | c28 |
| 35 | Reply-To | [26] 20.31 | o | o | [26] 20.31 | o | o |
| 36 | Require | [26] 20.32 | o | o | [26] 20.32 | m | m |
| 37 | Route | [26] 20.34 | m | m | [26] 20.34 | n/a | n/a |
| 38 | Security-Client | [48] 2.3.1 | c9 | c9 | [48] 2.3.1 | n/a | n/a |
| 39 | Security-Verify | [48] 2.3.1 | c10 | c10 | [48] 2.3.1 | n/a | n/a |
| 40 | SIP-If-Match | [70] 11.3.2 | o | o | [70] 11.3.2 | m | m |
| 41 | Subject | [26] 20.36 | o | o | [26] 20.36 | o | o |
| 42 | Supported | [26] 20.37, [26] 7.1 | o | o | [26] 20.37, [26] 7.1 | m | m |
| 43 | Timestamp | [26] 20.38 | c6 | c6 | [26] 20.38 | m | m |
| 44 | To | [26] 20.39 | m | m | [26] 20.39 | m | m |
| 45 | User-Agent | [26] 20.41 | o | o | [26] 20.41 | o | o |
| 46 | Via | [26] 20.42 | m | m | [26] 20.42 | m | m |

| | |
|---|---|
| c1: | IF A.4/20 THEN o ELSE n/a - - SIP specific event notification extension. |
| c2: | IF A.4/20 THEN m ELSE n/a - - SIP specific event notification extension. |
| c3: | IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA. |
| c4: | IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses. |
| c5: | IF A.4/8A THEN m ELSE n/a - - authentication between UA and proxy. |
| c6: | IF A.4/6 THEN o ELSE n/a - - timestamping of requests. |
| c7: | IF A.3/1 AND A.4/25 THEN o ELSE n/a - - UE and private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks. |
| c8: | IF A.4/38 THEN o ELSE n/a - - the Reason header field for the session initiation protocol. |
| c9: | IF A.4/37 THEN o ELSE n/a - - security mechanism agreement for the session initiation protocol (note 1). |
| c10: | IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. |
| c11: | IF A.4/25 THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks. |
| c12: | IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP). |
| c13: | IF A.4/32 THEN o ELSE n/a - - the P-Called-Party-ID extension. |
| c14: | IF A.4/33 THEN o ELSE n/a - - the P-Visited-Network-ID extension. |
| c15: | IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension. |
| c16: | IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE. |
| c17: | IF A.4/34 AND (A.3/7A OR A.3/7D) THEN m ELSE n/a - - the P-Access-Network-Info header extension and AS acting as terminating UA or AS acting as third-party call controller. |
| c18: | IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension. |
| c19: | IF A.4/36 THEN m ELSE n/a - - the P-Charging-Vector header extension. |
| c20: | IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension. |
| c21: | IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension. |
| c22: | IF A.4/40 THEN o ELSE n/a - - caller preferences for the session initiation protocol. |
| c25: | IF A.4/43 THEN m ELSE n/a - - the SIP Referred-By mechanism. |
| c26: | IF A.4/43 THEN o ELSE n/a - - the SIP Referred-By mechanism. |
| c28: | IF A.4/40 THEN m ELSE n/a - - caller preferences for the session initiation protocol. |
| NOTE 1: | Support of this header in this method is dependent on the security mechanism and the security architecture which is implemented. |
| NOTE 2: | The strength of this requirement in RFC 3455 [52] is SHOULD NOT, rather than MUST NOT. |

Prerequisite A.5/15A - - PUBLISH request

**Table A.104B: Supported message bodies within the PUBLISH request**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | | | | | | | |

Prerequisite A.5/15B - - PUBLISH response for all status-codes

**Table A.104C: Supported headers within the PUBLISH response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 0A | Allow | [26] 20.5 | c12 | c12 | [26] 20.5 | m | m |
| 1 | Call-ID | [26] 20.8 | m | m | [26] 20.8 | m | m |
| 2 | Call-Info | [26] 24.9 | o | o | [26] 24.9 | m | m |
| 3 | Content-Disposition | [26] 20.11 | o | o | [26] 20.11 | m | m |
| 4 | Content-Encoding | [26] 20.12 | o | o | [26] 20.12 | m | m |
| 5 | Content-Language | [26] 20.13 | o | o | [26] 20.13 | m | m |
| 6 | Content-Length | [26] 20.14 | m | m | [26] 20.14 | m | m |
| 7 | Content-Type | [26] 20.15 | m | m | [26] 20.15 | m | m |
| 8 | Cseq | [26] 20.16 | m | m | [26] 20.16 | m | m |
| 9 | Date | [26] 20.17 | c1 | c1 | [26] 20.17 | m | m |
| 10 | From | [26] 20.20 | m | m | [26] 20.20 | m | m |
| 11 | MIME-Version | [26] 20.24 | o | o | [26] 20.24 | m | m |
| 12 | Organization | [26] 20.25 | o | o | [26] 20.25 | o | o |
| 13 | P-Access-Network-Info | [52] 4.4 | c5 | c6 | [52] 4.4 | c5 | c7 |
| 14 | P-Asserted-Identity | [34] 9.1 | n/a | n/a | [34] 9.1 | c3 | c3 |
| 15 | P-Charging-Function-Addresses | [52] 4.5 | c10 | c11 | [52] 4.5 | c10 | c11 |
| 16 | P-Charging-Vector | [52] 4.6 | c8 | c9 | [52] 4.6 | c8 | c9 |
| 17 | P-Preferred-Identity | [34] 9.2 | c3 | x | [34] 9.2 | n/a | n/a |
| 18 | Privacy | [33] 4.2 | c4 | c4 | [33] 4.2 | c4 | c4 |
| 19 | Require | [26] 20.32 | m | m | [26] 20.32 | m | m |
| 20 | Server | [26] 20.35 | o | o | [26] 20.35 | o | o |
| 21 | Timestamp | [26] 20.38 | m | m | [26] 20.38 | c2 | c2 |
| 22 | To | [26] 20.39 | m | m | [26] 20.39 | m | m |
| 23 | User-Agent | [26] 20.41 | m | m | [26] 20.41 | i | i |
| 24 | Via | [26] 20.42 | m | m | [26] 20.42 | m | m |
| 25 | Warning | [26] 20.43 | o | o | [26] 20.43 | o | o |

c1: IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.
c2: IF A.4/6 THEN m ELSE n/a - - timestamping of requests.
c3: IF A.4/25 THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.
c4: IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c5: IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.
c6: IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE.
c7: IF A.4/34 AND (A.3/7A OR A.3/7D) THEN m ELSE n/a - - the P-Access-Network-Info header extension and AS acting as terminating UA or AS acting as third-party call controller.
c8: IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.
c9: IF A.4/36 THEN m ELSE n/a - - the P-Charging-Vector header extension.
c10: IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.
c11: IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.
c12: IF A.6/18 THEN m ELSE o - - 405 (Method Not Allowed)

NOTE: For a 488 (Not Acceptable Here) response, RFC 3261 [26] gives the status of this header as SHOULD rather than OPTIONAL.

Prerequisite A.5/15B - - PUBLISH response

Prerequisite: A.6/7 - - Additional for 200 (OK) response

**Table A.104D: Supported headers within the PUBLISH response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 2 | Authentication-Info | [26] 20.6 | c1 | c1 | [26] 20.6 | c2 | c2 |
| 3 | Expires | [26] 20.19, [70] 4, 5, 6 | m | m | [26] 20.19, [70] 4, 5, 6 | m | m |
| 4 | SIP-Etag | [70] 11.3.1 | m | m | [70] 11.3.1 | m | m |
| 5 | Supported | [26] 20.37 | m | m | [26] 20.37 | m | m |
| c1: IF A.4/7 THEN o ELSE n/a - - authentication between UA and UA.<br>c2: IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA. | | | | | | | |

Prerequisite A.5/15B - - PUBLISH response

Prerequisite: A.6/103 OR A.6/104 OR A.6/105 OR A.6/106 - - Additional for 3xx – 6xx response

**Table A.104DA: Supported headers within the PUBLISH response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Error-Info | [26] 20.18 | o | o | [26] 20.18 | o | o |

Prerequisite A.5/15B - - PUBLISH response

Prerequisite: A.6/103 OR A.6/35 - - Additional for 3xx or 485 (Ambiguous) response

**Table A.104E: Supported headers within the PUBLISH response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 2 | Contact | [26] 20.10 | o | o | [26] 20.10 | m | m |

Prerequisite A.5/15B - - PUBLISH response

Prerequisite: A.6/8 OR A.6/9 OR A.6/10 OR A.6/11OR A.6/12 – Additional for 401 (Unauthorized) response

**Table A.104F: Supported headers within the PUBLISH response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 3 | Proxy-Authenticate | [26] 20.27 | c1 | c1 | [26] 20.27 | c1 | c1 |
| 5 | WWW-Authenticate | [26] 20.44 | m | m | [26] 20.44 | m | m |
| c1: IF A.5/7 THEN m ELSE n/a - - support of authentication between UA and UA. | | | | | | | |

Prerequisite A.5/15B - - PUBLISH response

Prerequisite: A.6/17 OR A.6/23 OR A.6/30 OR A.6/36 OR A.6/42 OR A.6/45 OR A.6/50 OR A.6/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response

**Table A.104G: Supported headers within the PUBLISH response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 3 | Retry-After | [26] 20.33 | o | o | [26] 20.33 | o | o |

**Table A.104H: Void**

Prerequisite A.5/15B - - PUBLISH response

Prerequisite: A.6/20 - - Additional for 407 (Proxy Authentication Required) response

**Table A.104I: Supported headers within the PUBLISH response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 3 | Proxy-Authenticate | [26] 20.27 | c1 | c1 | [26] 20.27 | c1 | c1 |
| 5 | WWW-Authenticate | [26] 20.44 | o | o | [26] 20.44 | o | o |
| c1: | IF A.5/7 THEN m ELSE n/a - - support of authentication between UA and UA. | | | | | | |

Prerequisite A.5/15B - - PUBLISH response

Prerequisite: A.6/25 - - Additional for 415 (Unsupported Media Type) response

**Table A.104J: Supported headers within the PUBLISH response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Accept | [26] 20.1 | o.1 | o.1 | [26] 20.1 | m | m |
| 2 | Accept-Encoding | [26] 20.2 | o.1 | o.1 | [26] 20.2 | m | m |
| 3 | Accept-Language | [26] 20.3 | o.1 | o.1 | [26] 20.3 | m | m |
| o.1 | At least one of these capabilities is supported. | | | | | | |

Prerequisite A.5/15B - - PUBLISH response

Prerequisite: A.6/27 - - Additional for 420 (Bad Extension) response

**Table A.104K: Supported headers within the PUBLISH response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 4 | Unsupported | [26] 20.40 | m | m | [26] 20.40 | m | m |

Prerequisite A.5/15B - - PUBLISH response

Prerequisite: A.6/28 OR A.6/41A - - Additional for 421 (Extension Required), 494 (Security Agreement Required) response

**Table A.104L: Supported headers within the PUBLISH response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 3 | Security-Server | [48] 2 | x | x | [48] 2 | c1 | c1 |
| c1: | IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. | | | | | | |

Prerequisite A.5/15B - - PUBLISH response

Prerequisite: A.6/29 - - Additional for 423 (Interval Too Brief) response

**Table A.104M: Supported headers within the PUBLISH response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 3 | Min-Expires | [26] 20.23, [70] 5, 6 | m | m | [26] 20.23, [70] 5, 6 | m | m |

**Table A.104N: Void**

Prerequisite A.5/15B - - PUBLISH response

Prerequisite: A.6/39 - - Additional for 489 (Bad Event) response

**Table A.104O: Supported headers within the PUBLISH response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 2 | Allow-Events | [28] 8.2.2 | m | m | [28] 8.2.2 | m | m |

Prerequisite A.5/15B - - PUBLISH response

**Table A.104P: Supported message bodies within the PUBLISH response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | | | | | | | |

### A.2.1.4.11 REFER method

Prerequisite A.5/16 - - REFER request

**Table A.105: Supported headers within the REFER request**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 0A | Accept | [26] 20.1 | o | o | [26] 20.1 | m | m |
| 0B | Accept-Contact | [56B] 9.2 | c22 | c22 | [56B] 9.2 | c25 | c25 |
| 0C | Accept-Encoding | [26] 20.2 | o | o | [26] 20.2 | m | m |
| 1 | Accept-Language | [26] 20.3 | o | o | [26] 20.3 | m | m |
| 1A | Allow | [26] 20.5 | o | o | [26] 20.5 | m | m |
| 2 | Allow-Events | [28] 7.2.2 | c1 | c1 | [28] 7.2.2 | c2 | c2 |
| 3 | Authorization | [26] 20.7 | c3 | c3 | [26] 20.7 | c3 | c3 |
| 4 | Call-ID | [26] 20.8 | m | m | [26] 20.8 | m | m |
| 5 | Contact | [26] 20.10 | m | m | [26] 20.10 | m | m |
| 5A | Content-Disposition | [26] 20.11 | o | o | [26] 20.11 | m | m |
| 5B | Content-Encoding | [26] 20.12 | o | o | [26] 20.12 | m | m |
| 5C | Content-Language | [26] 20.13 | o | o | [26] 20.13 | m | m |
| 6 | Content-Length | [26] 20.14 | m | m | [26] 20.14 | m | m |
| 7 | Content-Type | [26] 20.15 | m | m | [26] 20.15 | m | m |
| 8 | Cseq | [26] 20.16 | m | m | [26] 20.16 | m | m |
| 9 | Date | [26] 20.17 | c4 | c4 | [26] 20.17 | m | m |
| 10 | Expires | [26] 20.19 | o | o | [26] 20.19 | o | o |
| 11 | From | [26] 20.20 | m | m | [26] 20.20 | m | m |
| 12 | Max-Forwards | [26] 20.22 | m | m | [26] 20.22 | n/a | n/a |
| 13 | MIME-Version | [26] 20.24 | o | o | [26] 20.24 | m | m |
| 14 | Organization | [26] 20.25 | o | o | [26] 20.25 | o | o |
| 14A | P-Access-Network-Info | [52] 4.4 | c12 | c13 | [52] 4.4 | c12 | c14 |
| 14B | P-Asserted-Identity | [34] 9.1 | n/a | n/a | [34] 9.1 | c8 | c8 |
| 14C | P-Called-Party-ID | [52] 4.2 | x | x | [52] 4.2 | c10 | c10 |
| 14D | P-Charging-Function-Addresses | [52] 4.5 | c17 | c18 | [52] 4.5 | c17 | c18 |
| 14E | P-Charging-Vector | [52] 4.6 | c15 | c16 | [52] 4.6 | c15 | c16 |
| 14F | P-Preferred-Identity | [34] 9.2 | c8 | c7 | [34] 9.2 | n/a | n/a |
| 14G | P-Visited-Network-ID | [52] 4.3 | x (note 1) | x | [52] 4.3 | c11 | n/a |
| 14H | Privacy | [33] 4.2 | c9 | c9 | [33] 4.2 | c9 | c9 |
| 15 | Proxy-Authorization | [26] 20.28 | c5 | c5 | [26] 20.28 | n/a | n/a |
| 16 | Proxy-Require | [26] 20.29 | o | n/a | [26] 20.29 | n/a | n/a |
| 16A | Reason | [34A] 2 | c21 | c21 | [34A] 2 | c21 | c21 |
| 17 | Record-Route | [26] 20.30 | n/a | n/a | [26] 20.30 | m | m |
| 18 | Refer-To | [36] 3 | m | m | [36] 3 | m | m |
| 18A | Referred-By | [59] 3 | c23 | c23 | [59] 3 | c23 | c23 |
| 18B | Reject-Contact | [56B] 9.2 | c22 | c22 | [56B] 9.2 | n/a | n/a |
| 18C | Request-Disposition | [56B] 9.1 | c22 | c22 | [56B] 9.1 | n/a | n/a |
| 19 | Require | [26] 20.32 | o | o | [26] 20.32 | m | m |
| 20 | Route | [26] 20.34 | m | m | [26] 20.34 | n/a | n/a |
| 20A | Security-Client | [48] 2.3.1 | c19 | c19 | [48] 2.3.1 | n/a | n/a |
| 20B | Security-Verify | [48] 2.3.1 | c20 | c20 | [48] 2.3.1 | n/a | n/a |
| 21 | Supported | [26] 20.37, [26] 7.1 | o | o | [26] 20.37, [26] 7.1 | m | m |
| 22 | Timestamp | [26] 20.38 | c6 | c6 | [26] 20.38 | m | m |
| 23 | To | [26] 20.39 | m | m | [26] 20.39 | m | m |
| 24 | User-Agent | [26] 20.41 | o | o | [26] 20.41 | o | o |
| 25 | Via | [26] 20.42 | m | m | [26] 20.42 | m | m |

| | |
|---|---|
| c1: | IF A.4/20 THEN o ELSE n/a - - SIP specific event notification extension. |
| c2: | IF A.4/20 THEN m ELSE n/a - - SIP specific event notification extension. |
| c3: | IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA. |
| c4: | IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses. |
| c5: | IF A.4/8A THEN m ELSE n/a - - authentication between UA and proxy. |
| c6: | IF A.4/6 THEN o ELSE n/a - - timestamping of requests. |
| c7: | IF A.3/1 AND A.4/25 THEN o ELSE n/a - - UE and private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks. |
| c8: | IF A.4/25 THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks. |
| c9: | IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP). |
| c10: | IF A.4/32 THEN o ELSE n/a - - the P-Called-Party-ID extension. |
| c11: | IF A.4/33 THEN o ELSE n/a - - the P-Visited-Network-ID extension. |
| c12: | IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension. |
| c13: | IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE. |
| c14: | IF A.4/34 AND (A.3/7A OR A.3/7D) THEN m ELSE n/a - - the P-Access-Network-Info header extension and AS acting as terminating UA or AS acting as third-party call controller. |
| c15: | IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension. |
| c16: | IF A.4/36 THEN m ELSE n/a - - the P-Charging-Vector header extension. |
| c17: | IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension. |
| c18: | IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension. |
| c19: | IF A.4/37 THEN o ELSE n/a - - security mechanism agreement for the session initiation protocol (note 2). |
| c20: | IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. |
| c21: | IF A.4/38 THEN o ELSE n/a - - the Reason header field for the session initiation protocol. |
| c22: | IF A.4/40 THEN o ELSE n/a - - caller preferences for the session initiation protocol. |
| c23: | IF A.4/43 THEN m ELSE n/a - - the SIP Referred-By Mechanism. |
| c25: | IF A.4/40 THEN m ELSE n/a - - caller preferences for the session initiation protocol. |
| NOTE 1: | The strength of this requirement in RFC 3455 [52] is SHOULD NOT, rather than MUST NOT. |
| NOTE 2: | Support of this header in this method is dependent on the security mechanism and the security architecture which is implemented. Use of this header in this method is not appropriate to the security mechanism defined by 3GPP TS 33.203 [19]. |

Prerequisite A.5/16 - - REFER request

**Table A.106: Supported message bodies within the REFER request**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | | | | | | | |

**Table A.107: Void**

Prerequisite A.5/17 - - REFER response for all status-codes

**Table A.108: Supported headers within the REFER response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 0A | Allow | [26] 20.5 | c12 | c12 | [26] 20.5 | m | m |
| 1 | Call-ID | [26] 20.8 | m | m | [26] 20.8 | m | m |
| 1A | Contact | [26] 20.10 | c13 | c13 | [26] 20.10 | m | m |
| 1B | Content-Disposition | [26] 20.11 | o | o | [26] 20.11 | m | m |
| 2 | Content-Encoding | [26] 20.12 | o | o | [26] 20.12 | m | m |
| 3 | Content-Language | [26] 20.13 | o | o | [26] 20.13 | m | m |
| 4 | Content-Length | [26] 20.14 | m | m | [26] 20.14 | m | m |
| 5 | Content-Type | [26] 20.15 | m | m | [26] 20.15 | m | m |
| 6 | Cseq | [26] 20.16 | m | m | [26] 20.16 | m | m |
| 7 | Date | [26] 20.17 | c1 | c1 | [26] 20.17 | m | m |
| 8 | From | [26] 20.20 | m | m | [26] 20.20 | m | m |
| 9 | MIME-Version | [26] 20.24 | o | o | [26] 20.24 | m | m |
| 10 | Organization | [26] 20.25 | o | o | [26] 20.25 | o | o |
| 10A | P-Access-Network-Info | [52] 4.4 | c5 | c6 | [52] 4.4 | c5 | c7 |
| 10B | P-Asserted-Identity | [34] 9.1 | n/a | n/a | [34] 9.1 | c3 | c3 |
| 10C | P-Charging-Function-Addresses | [52] 4.5 | c10 | c11 | [52] 4.5 | c10 | c11 |
| 10D | P-Charging-Vector | [52] 4.6 | c8 | c9 | [52] 4.6 | c8 | c9 |
| 10E | P-Preferred-Identity | [34] 9.2 | c3 | x | [34] 9.2 | n/a | n/a |
| 10F | Privacy | [33] 4.2 | c4 | c4 | [33] 4.2 | c4 | c4 |
| 10G | Require | [26] 20.32 | m | m | [26] 20.32 | m | m |
| 10H | Server | [26] 20.35 | o | o | [26] 20.35 | o | o |
| 11 | Timestamp | [26] 20.38 | m | m | [26] 20.38 | c2 | c2 |
| 12 | To | [26] 20.39 | m | m | [26] 20.39 | m | m |
| 12A | User-Agent | [26] 20.41 | o | o | [26] 20.41 | o | o |
| 13 | Via | [26] 20.42 | m | m | [26] 20.42 | m | m |
| 14 | Warning | [26] 20.43 | o (note) | o | [26] 20.43 | o | o |
| c1: | IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses. | | | | | | |
| c2: | IF A.4/6 THEN m ELSE n/a - - timestamping of requests. | | | | | | |
| c3: | IF A.4/25 THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks. | | | | | | |
| c4: | IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP). | | | | | | |
| c5: | IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension. | | | | | | |
| c6: | IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE. | | | | | | |
| c7: | IF A.4/34 AND (A.3/7A OR A.3/7D) THEN m ELSE n/a - - the P-Access-Network-Info header extension and AS acting as terminating UA or AS acting as third-party call controller. | | | | | | |
| c8: | IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension. | | | | | | |
| c9: | IF A.4/36 THEN m ELSE n/a - - the P-Charging-Vector header extension. | | | | | | |
| c10: | IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension. | | | | | | |
| c11: | IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension. | | | | | | |
| c12: | IF A.6/18 THEN m ELSE o - - 405 (Method Not Allowed) | | | | | | |
| c13: | IF A.6/102 THEN m ELSE o - - 2xx response | | | | | | |
| NOTE: | For a 488 (Not Acceptable Here) response, RFC 3261 [26] gives the status of this header as SHOULD rather than OPTIONAL. | | | | | | |

Prerequisite A.5/17 - - REFER response

Prerequisite: A.6/102 - - Additional for 2xx response

**Table A.109: Supported headers within the REFER response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Allow-Events | [28] 7.2.2 | c3 | c3 | [28] 7.2.2 | c4 | c4 |
| 2 | Authentication-Info | [26] 20.6 | c1 | c1 | [26] 20.6 | c2 | c2 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 5 | Record-Route | [26] 20.30 | m | m | [26] 20.30 | m | m |
| 8 | Supported | [26] 20.37 | m | m | [26] 20.37 | m | m |
| c1: | IF A.4/7 THEN o ELSE n/a - - authentication between UA and UA. | | | | | | |
| c2: | IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA. | | | | | | |
| c3: | IF A.4/20 THEN o ELSE n/a - - SIP specific event notification extension. | | | | | | |
| c4: | IF A.4/20 THEN m ELSE n/a - - SIP specific event notification extension. | | | | | | |

Prerequisite A.5/17 - - REFER response

Prerequisite: A.6/103 OR A.6/104 OR A.6/105 OR A.6/106 - - Additional for 3xx – 6xx response

**Table A.109A: Supported headers within the REFER response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Error-Info | [26] 20.18 | o | o | [26] 20.18 | o | o |

**Table A.110: Void**

Prerequisite A.5/17 - - REFER response

Prerequisite: A.6/14 - - Additional for 401 (Unauthorized) response

**Table A.111: Supported headers within the REFER response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 4 | Proxy-Authenticate | [26] 20.27 | c1 | c1 | [26] 20.27 | c1 | c1 |
| 10 | WWW-Authenticate | [26] 20.44 | m | m | [26] 20.44 | m | m |
| c1: | IF A.5/7 THEN m ELSE n/a - - support of authentication between UA and UA. | | | | | | |

Prerequisite A.5/17 - - REFER response

Prerequisite: A.6/17 OR A.6/23 OR A.6/30 OR A.6/36 OR A.6/42 OR A.6/45 OR A.6/50 OR A.6/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response

**Table A.112: Supported headers within the REFER response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 6 | Retry-After | [26] 20.33 | o | o | [26] 20.33 | o | o |

**Table A.113: Void**

Prerequisite A.5/17 - - REFER response

Prerequisite: A.6/20 - - Additional for 407 (Proxy Authentication Required) response

**Table A.114: Supported headers within the REFER response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 4 | Proxy-Authenticate | [26] 20.27 | c1 | c1 | [26] 20.27 | c1 | c1 |
| 8 | WWW-Authenticate | [26] 20.44 | o | o | [26] 20.44 | o | o |
| c1: | IF A.5/7 THEN m ELSE n/a - - support of authentication between UA and UA. | | | | | | |

Prerequisite A.5/17 - - REFER response

Prerequisite: A.6/25 - - Additional for 415 (Unsupported Media Type) response

**Table A.115: Supported headers within the REFER response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Accept | [26] 20.1 | o.1 | o.1 | [26] 20.1 | m | m |
| 2 | Accept-Encoding | [26] 20.2 | o.1 | o.1 | [26] 20.2 | m | m |
| 3 | Accept-Language | [26] 20.3 | o.1 | o.1 | [26] 20.3 | m | m |
| o.1 | At least one of these capabilities is supported. | | | | | | |

Prerequisite A.5/17 - - REFER response

Prerequisite: A.6/27 - - Additional for 420 (Bad Extension) response

**Table A.116: Supported headers within the REFER response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 8 | Unsupported | [26] 20.40 | m | m | [26] 20.40 | m | m |

Prerequisite A.5/17 - - REFER response

Prerequisite: A.6/28 OR A.6/41A - - Additional for 421 (Extension Required), 494 (Security Agreement Required) response

**Table A.116A: Supported headers within the REFER response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 3 | Security-Server | [48] 2 | x | x | [48] 2 | c1 | c1 |
| c1: | IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. | | | | | | |

**Table A.117: Void**

Prerequisite A.5/17 - - REFER response

**Table A.118: Supported message bodies within the REFER response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | | | | | | | |

### A.2.1.4.12 REGISTER method

Prerequisite A.5/18 - - REGISTER request

**Table A.119: Supported headers within the REGISTER request**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Accept | [26] 20.1 | o | o | [26] 20.1 | m | m |
| 2 | Accept-Encoding | [26] 20.2 | o | o | [26] 20.2 | m | m |
| 3 | Accept-Language | [26] 20.3 | o | o | [26] 20.3 | m | m |
| 3A | Allow | [26] 20.5 | o | o | [26] 20.5 | m | m |
| 4 | Allow-Events | [28] 7.2.2 | c27 | c27 | [28] 7.2.2 | c1 | c1 |
| 5 | Authorization | [26] 20.7, [49] | c2 | o | [26] 20.7, [49] | m | c22 |
| 6 | Call-ID | [26] 20.8 | m | m | [26] 20.8 | m | m |
| 7 | Call-Info | [26] 20.9 | o | o | [26] 20.9 | o | o |
| 8 | Contact | [26] 20.10 | o | m | [26] 20.10 | m | m |
| 9 | Content-Disposition | [26] 20.11 | o | o | [26] 20.11 | m | m |
| 10 | Content-Encoding | [26] 20.12 | o | o | [26] 20.12 | m | m |
| 11 | Content-Language | [26] 20.13 | o | o | [26] 20.13 | m | m |
| 12 | Content-Length | [26] 20.14 | m | m | [26] 20.14 | m | m |
| 13 | Content-Type | [26] 20.15 | m | m | [26] 20.15 | m | m |
| 14 | Cseq | [26] 20.16 | m | m | [26] 20.16 | m | m |
| 15 | Date | [26] 20.17 | c3 | c3 | [26] 20.17 | m | m |
| 16 | Expires | [26] 20.19 | o | o | [26] 20.19 | m | m |
| 17 | From | [26] 20.20 | m | m | [26] 20.20 | m | m |
| 18 | Max-Forwards | [26] 20.22 | m | m | [26] 20.22 | n/a | n/a |
| 19 | MIME-Version | [26] 20.24 | o | o | [26] 20.24 | m | m |
| 20 | Organization | [26] 20.25 | o | o | [26] 20.25 | o | o |
| 20A | P-Access-Network-Info | [52] 4.4 | c12 | c13 | [52] 4.4 | c12 | c14 |
| 20B | P-Charging-Function-Addresses | [52] 4.5 | c17 | c18 | [52] 4.5 | c17 | c18 |
| 20C | P-Charging-Vector | [52] 4.6 | c15 | c16 | [52] 4.6 | c15 | c16 |
| 20D | P-Visited-Network-ID | [52] 4.3 | x (note 2) | x | [52] 4.3 | c10 | c11 |
| 20E | Path | [35] 4 | c4 | c5 | [35] 4 | m | c6 |
| 20F | Privacy | [33] 4.2 | c9 | n/a | [33] 4.2 | c9 | n/a |
| 21 | Proxy-Authorization | [26] 20.28 | c8 | c8 | [26] 20.28 | n/a | n/a |
| 22 | Proxy-Require | [26] 20.29 | o | o (note 1) | [26] 20.29 | n/a | n/a |
| 22A | Reason | [34A] 2 | c23 | c23 | [34A] 2 | c23 | c23 |
| 22B | Referred-By | [59] 3 | c25 | c25 | [59] 3 | c26 | c26 |
| 22C | Request-Disposition | [56B] 9.1 | c24 | c24 | [56B] 9.1 | n/a | n/a |
| 23 | Require | [26] 20.32 | o | o | [26] 20.32 | m | m |
| 24 | Route | [26] 20.34 | o | n/a | [26] 20.34 | n/a | n/a |
| 24A | Security-Client | [48] 2.3.1 | c19 | c20 | [48] 2.3.1 | n/a | n/a |
| 24B | Security-Verify | [48] 2.3.1 | c20 | c20 | [48] 2.3.1 | c21 | n/a |
| 25 | Supported | [26] 20.37 | o | c28 | [26] 20.37 | m | m |
| 26 | Timestamp | [26] 20.38 | c7 | c7 | [26] 20.38 | c7 | c7 |
| 27 | To | [26] 20.39 | m | m | [26] 20.39 | m | m |
| 28 | User-Agent | [26] 20.41 | o | o | [26] 20.41 | o | o |
| 29 | Via | [26] 20.42 | m | m | [26] 20.42 | m | m |

| | |
|---|---|
| c1: | IF A.4/20 THEN m ELSE n/a - - SIP specific event notification extension. |
| c2: | IF A.4/8 THEN m ELSE n/a - - authentication between UA and registrar. |
| c3: | IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses. |
| c4: | IF A.4/24 THEN o ELSE n/a - - session initiation protocol extension header field for registering non-adjacent contacts. |
| c5: | IF A.4/24 THEN x ELSE n/a - - session initiation protocol extension header field for registering non-adjacent contacts. |
| c6: | IF A.3/4 THEN m ELSE n/a. - - S-CSCF. |
| c7: | IF A.4/6 THEN m ELSE n/a - - timestamping of requests. |
| c8: | IF A.4/8A THEN m ELSE n/a - - authentication between UA and proxy. |
| c9: | IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP). |
| c10: | IF A.4/33 THEN o ELSE n/a - - the P-Visited-Network-ID extension. |
| c11: | IF A.4/33 THEN m ELSE n/a - - the P-Visited-Network-ID extension. |
| c12: | IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension. |
| c13: | IF A.4/34 AND (A.3/1 OR A.3/4) THEN o ELSE n/a - - the P-Access-Network-Info header extension and UE or S-CSCF. |
| c14: | IF A.4/34 AND (A.3/4 OR A.3/7A) THEN m ELSE n/a - - the P-Access-Network-Info header extension and S-CSCF or AS acting as terminating UA. |
| c15: | IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension. |
| c16: | IF A.4/36 OR A.3/4 THEN m ELSE n/a - - the P-Charging-Vector header extension (including S-CSCF as registrar). |
| c17: | IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension. |
| c18: | IF A.4/35 OR A.3/4 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension (including S-CSCF as registrar). |
| c19: | IF A.4/37 THEN o ELSE n/a - - security mechanism agreement for the session initiation protocol (note 3). |
| c20: | IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. |
| c21: | IF A.4/37 AND A.4/2 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol and registrar. |
| c22: | IF A.3/4 THEN m ELSE n/a - - S-CSCF. |
| c23: | IF A.4/38 THEN o ELSE n/a - - the Reason header field for the session initiation protocol. |
| c24: | IF A.4/40 THEN o ELSE n/a - - caller preferences for the session initiation protocol. |
| c25: | IF A.4/43 THEN m ELSE n/a - - the SIP Referred-By mechanism. |
| c26: | IF A.4/43 THEN o ELSE n/a - - the SIP Referred-By mechanism. |
| c27: | IF A.4/20 THEN o ELSE n/a - - SIP specific event notification extension. |
| c28: | IF A.3/1 THEN m ELSE o - - UE. |
| NOTE 1: | No distinction has been made in these tables between first use of a request on a From/To/Call-ID combination, and the usage in a subsequent one. Therefore the use of "o" etc. above has been included from a viewpoint of first usage. |
| NOTE 2: | The strength of this requirement in RFC 3455 [52] is SHOULD NOT, rather than MUST NOT. |
| NOTE 3: | Support of this header in this method is dependent on the security mechanism and the security architecture which is implemented. |

Prerequisite A.5/18 - - REGISTER request

**Table A.120: Supported message bodies within the REGISTER request**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | | | | | | | |

**Table A.121: Void**

Prerequisite A.5/19 - - REGISTER response for all status-codes

**Table A.122: Supported headers within the REGISTER response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 0A | Allow | [26] 20.5 | c8 | c8 | [26] 20.5 | m | m |
| 1 | Call-ID | [26] 20.8 | m | m | [26] 20.8 | m | m |
| 1A | Call-Info | [26] 20.9 | o | o | [26] 20.9 | o | o |
| 2 | Content-Disposition | [26] 20.11 | o | o | [26] 20.11 | m | m |
| 3 | Content-Encoding | [26] 20.12 | o | o | [26] 20.12 | m | m |
| 4 | Content-Language | [26] 20.13 | o | o | [26] 20.13 | m | m |
| 5 | Content-Length | [26] 20.14 | m | m | [26] 20.14 | m | m |
| 6 | Content-Type | [26] 20.15 | m | m | [26] 20.15 | m | m |
| 7 | Cseq | [26] 20.16 | m | m | [26] 20.16 | m | m |
| 8 | Date | [26] 20.17 | c1 | c1 | [26] 20.17 | m | m |
| 9 | From | [26] 20.20 | m | m | [26] 20.20 | m | m |
| 10 | MIME-Version | [26] 20.24 | o | o | [26] 20.24 | m | m |
| 11 | Organization | [26] 20.25 | o | o | [26] 20.25 | o | o |
| 11A | P-Access-Network-Info | [52] 4.4 | c3 | n/a | [52] 4.4 | c3 | n/a |
| 11B | P-Charging-Function-Addresses | [52] 4.5 | c6 | c7 | [52] 4.5 | c6 | c7 |
| 11C | P-Charging-Vector | [52] 4.6 | c4 | c5 | [52] 4.6 | c4 | c5 |
| 11D | Privacy | [33] 4.2 | c2 | n/a | [33] 4.2 | c2 | n/a |
| 11E | Require | [26] 20.32 | m | m | [26] 20.32 | m | m |
| 11F | Server | [26] 20.35 | o | o | [26] 20.35 | o | o |
| 12 | Timestamp | [26] 20.38 | c2 | c2 | [26] 20.38 | m | m |
| 13 | To | [26] 20.39 | m | m | [26] 20.39 | m | m |
| 13A | User-Agent | [26] 20.41 | o | o | [26] 20.41 | o | o |
| 14 | Via | [26] 20.42 | m | m | [26] 20.42 | m | m |
| 15 | Warning | [26] 20.43 | o (note) | o | [26] 20.43 | o | o |

c1: IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.
c2: IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c3: IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.
c4: IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.
c5: IF A.4/36 OR A.3/4 THEN m ELSE n/a - - the P-Charging-Vector header extension (including S-CSCF as registrar).
c6: IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.
c7: IF A.4/35 OR A.3/4 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension (including S-CSCF as registrar).
c8: IF A.6/18 THEN m ELSE o - - 405 (Method Not Allowed)

NOTE: For a 488 (Not Acceptable Here) response, RFC 3261 [26] gives the status of this header as SHOULD rather than OPTIONAL.

Prerequisite A.5/19 - - REGISTER response

Prerequisite: A.6/102 - - Additional for 2xx response

**Table A.123: Supported headers within the REGISTER response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Accept | [26] 20.1 | o | | [26] 20.1 | o | |
| 1A | Accept-Encoding | [26] 20.2 | o | o | [26] 20.2 | m | m |
| 1B | Accept-Language | [26] 20.3 | o | o | [26] 20.3 | m | m |
| 2 | Allow-Events | [28] 7.2.2 | c12 | c12 | [28] 7.2.2 | c13 | c13 |
| 3 | Authentication-Info | [26] 20.6 | c6 | c6 | [26] 20.6 | c7 | c7 |
| 5 | Contact | [26] 20.10 | o | o | [26] 20.10 | m | m |
| 5A | P-Associated-URI | [52] 4.1 | c8 | c9 | [52] 4.1 | c10 | c11 |
| 6 | Path | [35] 4 | c3 | c3 | [35] 4 | c4 | c4 |
| 8 | Service-Route | [38] 5 | c5 | c5 | [38] 5 | c5 | c5 |
| 9 | Supported | [26] 20.37 | m | m | [26] 20.37 | m | m |
| c1: | IF (A.3/4 AND A.4/2) THEN m ELSE n/a. - - S-CSCF acting as registrar. | | | | | | |
| c2: | IF A.3/4 OR A.3/1THEN m ELSE n/a. - - S-CSCF or UE. | | | | | | |
| c3: | IF A.4/24 THEN m ELSE n/a - - session initiation protocol extension header field for registering non-adjacent contacts. | | | | | | |
| c4: | IF A.4/24 THEN o ELSE n/a - - session initiation protocol extension header field for registering non-adjacent contacts. | | | | | | |
| c5: | IF A.4/28 THEN m ELSE n/a - - session initiation protocol extension header field for service route discovery during registration. | | | | | | |
| c6: | IF A.4/8 THEN o ELSE n/a - - authentication between UA and registrar. | | | | | | |
| c7: | IF A.4/8 THEN m ELSE n/a - - authentication between UA and registrar. | | | | | | |
| c8: | IF A.4/2 AND A.4/31 THEN m ELSE n/a - - P-Assocated-URI header extension and registrar. | | | | | | |
| c9: | IF A.3/1 AND A.4/31 THEN m ELSE n/a - - P-Assocated-URI header extension and S-CSCF. | | | | | | |
| c10: | IF A.4/31 THEN o ELSE n/a - - P-Assocated-URI header extension. | | | | | | |
| c11: | IF A.4/31 AND A.3/1 THEN m ELSE n/a - - P-Assocated-URI header extension and UE. | | | | | | |
| c12: | IF A.4/20 THEN o ELSE n/a - - SIP specific event notification extension. | | | | | | |
| c13: | IF A.4/20 THEN m ELSE n/a - - SIP specific event notification extension. | | | | | | |

Prerequisite A.5/19 - - REGISTER response

Prerequisite: A.6/103 OR A.6/104 OR A.6/105 OR A.6/106 - - Additional for 3xx – 6xx response

**Table A.123A: Supported headers within the REGISTER response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Error-Info | [26] 20.18 | o | o | [26] 20.18 | o | o |

Prerequisite A.5/19 - - REGISTER response

Prerequisite: A.6/103 OR A.6/35 - - Additional for 3xx or 485 (Ambiguous) response

**Table A.124: Supported headers within the REGISTER response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 3 | Contact | [26] 20.10 | o (note) | o | [26] 20.10 | m | m |

Prerequisite A.5/19 - - REGISTER response

Prerequisite: A.6/14 - - Additional for 401 (Unauthorized) response

**Table A.125: Supported headers within the REGISTER response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 4 | Proxy-Authenticate | [26] 20.27 | c1 | x | [26] 20.27 | c1 | x |
| 6 | Security-Server | [48] 2 | x | x | [48] 2 | n/a | c2 |
| 10 | WWW-Authenticate | [26] 20.44 | m | m | [26] 20.44 | m | m |
| c1: | IF A.5/8 THEN m ELSE n/a - - support of authentication between UA and UA. | | | | | | |
| c2: | IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. | | | | | | |

Prerequisite A.5/19 - - REGISTER response

Prerequisite: A.6/17 OR A.6/23 OR A.6/30 OR A.6/36 OR A.6/42 OR A.6/45 OR A.6/50 OR A.6/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response

**Table A.126: Supported headers within the REGISTER response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 6 | Retry-After | [26] 20.33 | o | o | [26] 20.33 | o | o |

**Table A.127: Void**

Prerequisite A.5/19 - - REGISTER response

Prerequisite: A.6/20 - - Additional for 407 (Proxy Authentication Required) response

**Table A.128: Supported headers within the REGISTER response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 5 | Proxy-Authenticate | [26] 20.27 | c1 | x | [26] 20.27 | c1 | x |
| 9 | WWW-Authenticate | [26] 20.44 | o | o | [26] 20.44 | o | o |
| c1: | IF A.5/8 THEN m ELSE n/a - - support of authentication between UA and UA. | | | | | | |

Prerequisite A.5/19 - - REGISTER response

Prerequisite: A.6/25 - - Additional for 415 (Unsupported Media Type) response

**Table A.129: Supported headers within the REGISTER response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Accept | [26] 20.1 | o.1 | o.1 | [26] 20.1 | m | m |
| 2 | Accept-Encoding | [26] 20.2 | o.1 | o.1 | [26] 20.2 | m | m |
| 3 | Accept-Language | [26] 20.3 | o.1 | o.1 | [26] 20.3 | m | m |
| o.1 | At least one of these capabilities is supported. | | | | | | |

Prerequisite A.5/19 - - REGISTER response

Prerequisite: A.6/27 - - Additional for 420 (Bad Extension) response

**Table A.130: Supported headers within the REGISTER response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 8 | Unsupported | [26] 20.40 | m | m | [26] 20.40 | m | m |

Prerequisite A.5/19 - - REGISTER response

Prerequisite: A.6/28 OR A.6/41A - - Additional for 421 (Extension Required), 494 (Security Agreement Required) response

**Table A.130A: Supported headers within the REGISTER response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 3 | Security-Server | [48] 2 | c2 | c2 | [48] 2 | c1 | c1 |
| c1: | IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. | | | | | | |
| c2: | IF A.4/37 AND A.4/2 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol and registrar. | | | | | | |

Prerequisite A.5/19 - - REGISTER response

Prerequisite: A.6/29 - - Additional for 423 (Interval Too Brief) response

**Table A.131: Supported headers within the REGISTER response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 5 | Min-Expires | [26] 20.23 | m | m | [26] 20.23 | m | m |

**Table A.132: Void**

Prerequisite A.5/19 - - REGISTER response

**Table A.133: Supported message bodies within the REGISTER response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | | | | | | | |

### A.2.1.4.13 SUBSCRIBE method

Prerequisite A.5/20 - - SUBSCRIBE request

**Table A.134: Supported headers within the SUBSCRIBE request**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Accept | [26] 20.1 | o | o | [26] 20.1 | m | m |
| 1A | Accept-Contact | [56B] 9.2 | c22 | c22 | [56B] 9.2 | c26 | c26 |
| 2 | Accept-Encoding | [26] 20.2 | o | o | [26] 20.2 | m | m |
| 3 | Accept-Language | [26] 20.3 | o | o | [26] 20.3 | m | m |
| 3A | Allow | [26] 20.5 | o | o | [26] 20.5 | m | m |
| 4 | Allow-Events | [28] 7.2.2 | o | o | [28] 7.2.2 | m | m |
| 5 | Authorization | [26] 20.7 | c3 | c3 | [26] 20.7 | c3 | c3 |
| 6 | Call-ID | [26] 20.8 | m | m | [26] 20.8 | m | m |
| 6A | Contact | [26] 20.10 | m | m | [26] 20.10 | m | m |
| 7 | Content-Disposition | [26] 20.11 | o | o | [26] 20.11 | m | m |
| 8 | Content-Encoding | [26] 20.12 | o | o | [26] 20.12 | m | m |
| 9 | Content-Language | [26] 20.13 | o | o | [26] 20.13 | m | m |
| 10 | Content-Length | [26] 20.14 | m | m | [26] 20.14 | m | m |
| 11 | Content-Type | [26] 20.15 | m | m | [26] 20.15 | m | m |
| 12 | Cseq | [26] 20.16 | m | m | [26] 20.16 | m | m |
| 13 | Date | [26] 20.17 | c4 | c4 | [26] 20.17 | m | m |
| 14 | Event | [28] 7.2.1 | m | m | [28] 7.2.1 | m | m |
| 15 | Expires | [26] 20.19 | o (note 1) | o (note 1) | [26] 20.19 | m | m |
| 16 | From | [26] 20.20 | m | m | [26] 20.20 | m | m |
| 17 | Max-Forwards | [26] 20.22 | m | m | [26] 20.22 | n/a | n/a |
| 18 | MIME-Version | [26] 20.24 | o | o | [26] 20.24 | m | m |
| 18A | Organization | [26] 20.25 | o | o | [26] 20.25 | o | o |
| 18B | P-Access-Network-Info | [52] 4.4 | c12 | c13 | [52] 4.4 | c12 | c14 |
| 18C | P-Asserted-Identity | [34] 9.1 | n/a | n/a | [34] 9.1 | c6 | c6 |
| 18D | P-Called-Party-ID | [52] 4.2 | x | x | [52] 4.2 | c10 | c10 |
| 18E | P-Charging-Function-Addresses | [52] 4.5 | c17 | c18 | [52] 4.5 | c17 | c18 |
| 18F | P-Charging-Vector | [52] 4.6 | c15 | c16 | [52] 4.6 | c15 | c16 |
| 18G | P-Preferred-Identity | [34] 9.2 | c6 | c7 | [34] 9.2 | n/a | n/a |
| 18H | P-Visited-Network-ID | [52] 4.3 | x (note 2) | x | [52] 4.3 | c11 | n/a |
| 18I | Privacy | [33] 4.2 | c9 | c9 | [33] 4.2 | c9 | c9 |
| 19 | Proxy-Authorization | [26] 20.28 | c5 | c5 | [26] 20.28 | n/a | n/a |
| 20 | Proxy-Require | [26] 20.29 | o | n/a | [26] 20.29 | n/a | n/a |
| 20A | Reason | [34A] 2 | c21 | c21 | [34A] 2 | c21 | c21 |
| 21 | Record-Route | [26] 20.30 | n/a | n/a | [26] 20.30 | m | m |
| 21A | Referred-By | [59] 3 | c23 | c23 | [59] 3 | c24 | c24 |
| 21B | Reject-Contact | [56B] 9.2 | c22 | c22 | [56B] 9.2 | c26 | c26 |
| 21C | Request-Disposition | [56B] 9.1 | c22 | c22 | [56B] 9.1 | c26 | c26 |
| 22 | Require | [26] 20.32 | o | o | [26] 20.32 | m | m |
| 23 | Route | [26] 20.34 | m | m | [26] 20.34 | n/a | n/a |
| 23A | Security-Client | [48] 2.3.1 | c19 | c19 | [48] 2.3.1 | n/a | n/a |
| 23B | Security-Verify | [48] 2.3.1 | c20 | c20 | [48] 2.3.1 | n/a | n/a |
| 24 | Supported | [26] 20.37 | o | o | [26] 20.37 | m | m |
| 25 | Timestamp | [26] 20.38 | c8 | c8 | [26] 20.38 | m | m |
| 26 | To | [26] 20.39 | m | m | [26] 20.39 | m | m |
| 27 | User-Agent | [26] 20.41 | o | o | [26] 20.41 | o | o |
| 28 | Via | [26] 20.42 | m | m | [26] 20.42 | m | m |

| | |
|---|---|
| c3: | IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA. |
| c4: | IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses. |
| c5: | IF A.4/8A THEN m ELSE n/a - - authentication between UA and proxy. |
| c6: | IF A.4/25 THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks. |
| c7: | IF A.3/1 AND A.4/25 THEN o ELSE n/a - - UE and private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks. |
| c8: | IF A.4/6 THEN o ELSE n/a - - timestamping of requests. |
| c9: | IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP). |
| c10: | IF A.4/32 THEN o ELSE n/a - - the P-Called-Party-ID extension. |
| c11: | IF A.4/33 THEN o ELSE n/a - - the P-Visited-Network-ID extension. |
| c12: | IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension. |
| c13: | IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE. |
| c14: | IF A.4/34 AND (A.3/7A OR A.3/7D) THEN m ELSE n/a - - the P-Access-Network-Info header extension and AS acting as terminating UA or AS acting as third-party call controller. |
| c15: | IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension. |
| c16: | IF A.4/36 THEN m ELSE n/a - - the P-Charging-Vector header extension. |
| c17: | IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension. |
| c18: | IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension. |
| c19: | IF A.4/37 THEN o ELSE n/a - - security mechanism agreement for the session initiation protocol (note 3). |
| c20: | IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. |
| c21: | IF A.4/38 THEN o ELSE n/a - - the Reason header field for the session initiation protocol. |
| c22: | IF A.4/40 THEN o ELSE n/a - - caller preferences for the session initiation protocol. |
| c23: | IF A.4/43 THEN m ELSE n/a - - the SIP Referred-By mechanism. |
| c24: | IF A.4/43 THEN o ELSE n/a - - the SIP Referred-By mechanism. |
| c26: | IF A.4/40 THEN m ELSE n/a - - caller preferences for the session initiation protocol. |
| NOTE 1: | The strength of this requirement is RECOMMENDED rather than OPTIONAL. |
| NOTE 2: | The strength of this requirement in RFC 3455 [52] is SHOULD NOT, rather than MUST NOT. |
| NOTE 3: | Support of this header in this method is dependent on the security mechanism and the security architecture which is implemented. Use of this header in this method is not appropriate to the security mechanism defined by 3GPP TS 33.203 [19]. |

Prerequisite A.5/20 - - SUBSCRIBE request

**Table A.135: Supported message bodies within the SUBSCRIBE request**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | | | | | | | |

Prerequisite A.5/21 - - SUBSCRIBE response for all status-codes

**Table A.136: Supported headers within the SUBSCRIBE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 0A | Allow | [26] 20.5 | c12 | c12 | [26] 20.5 | m | m |
| 1 | Call-ID | [26] 20.8 | m | m | [26] 20.8 | m | m |
| 2 | Content-Disposition | [26] 20.11 | o | o | [26] 20.11 | m | m |
| 3 | Content-Encoding | [26] 20.12 | o | o | [26] 20.12 | m | m |
| 4 | Content-Language | [26] 20.13 | o | o | [26] 20.13 | m | m |
| 5 | Content-Length | [26] 20.14 | m | m | [26] 20.14 | m | m |
| 6 | Content-Type | [26] 20.15 | m | m | [26] 20.15 | m | m |
| 7 | Cseq | [26] 20.16 | m | m | [26] 20.16 | m | m |
| 8 | Date | [26] 20.17 | c1 | c1 | [26] 20.17 | m | m |
| 9 | From | [26] 20.20 | m | m | [26] 20.20 | m | m |
| 10 | MIME-Version | [26] 20.24 | o | o | [26] 20.24 | m | m |
| 10A | Organization | [26] 20.25 | o | o | [26] 20.25 | o | o |
| 10B | P-Access-Network-Info | [52] 4.4 | c5 | c6 | [52] 4.4 | c5 | c7 |
| 10C | P-Asserted-Identity | [34] 9.1 | n/a | n/a | [34] 9.1 | c3 | c3 |
| 10D | P-Charging-Function-Addresses | [52] 4.5 | c10 | c11 | [52] 4.5 | c10 | c11 |
| 10E | P-Charging-Vector | [52] 4.6 | c8 | c9 | [52] 4.6 | c8 | c9 |
| 10F | P-Preferred-Identity | [34] 9.2 | c3 | x | [34] 9.2 | n/a | n/a |
| 10G | Privacy | [33] 4.2 | c4 | c4 | [33] 4.2 | c4 | c4 |
| 10H | Require | [26] 20.32 | m | m | [26] 20.32 | m | m |
| 10I | Server | [26] 20.35 | o | o | [26] 20.35 | o | o |
| 11 | Timestamp | [26] 20.38 | m | m | [26] 20.38 | c2 | c2 |
| 12 | To | [26] 20.39 | m | m | [26] 20.39 | m | m |
| 12A | User-Agent | [26] 20.41 | o | o | [26] 20.41 | o | o |
| 13 | Via | [26] 20.42 | m | m | [26] 20.42 | m | m |
| 14 | Warning | [26] 20.43 | o (note) | o | [26] 20.43 | o | o |
| c1: | IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses. | | | | | | |
| c2: | IF A.4/6 THEN m ELSE n/a - - timestamping of requests. | | | | | | |
| c3: | IF A.4/25 THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks. | | | | | | |
| c4: | IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP). | | | | | | |
| c5: | IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension. | | | | | | |
| c6: | IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE. | | | | | | |
| c7: | IF A.4/34 AND (A.3/7A OR A.3/7D) THEN m ELSE n/a - - the P-Access-Network-Info header extension and AS acting as terminating UA or AS acting as third-party call controller. | | | | | | |
| c8: | IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension. | | | | | | |
| c9: | IF A.4/36 THEN m ELSE n/a - - the P-Charging-Vector header extension. | | | | | | |
| c10: | IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension. | | | | | | |
| c11: | IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension. | | | | | | |
| c12: | IF A.6/18 THEN m ELSE o - - 405 (Method Not Allowed) | | | | | | |
| NOTE: | For a 488 (Not Acceptable Here) response, RFC 3261 [26] gives the status of this header as SHOULD rather than OPTIONAL. | | | | | | |

Prerequisite A.5/21 - - SUBSCRIBE response

Prerequisite: A.6/102 - - Additional for 2xx response

**Table A.137: Supported headers within the SUBSCRIBE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 0A | Allow-Events | [28] 7.2.2 | o | o | [28] 7.2.2 | m | m |
| 1 | Authentication-Info | [26] 20.6 | c1 | c1 | [26] 20.6 | c2 | c2 |
| 1A | Contact | [26] 20.10 | m | m | [26] 20.10 | m | m |
| 2 | Expires | [26] 20.19 | m | m | [26] 20.19 | m | m |
| 4 | Require | [26] 20.32 | m | m | [26] 20.32 | m | m |
| 6 | Supported | [26] 20.37 | m | m | [26] 20.37 | m | m |

| | |
|---|---|
| c1: | IF A.4/7 THEN o ELSE n/a - - authentication between UA and UA. |
| c2: | IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA. |

Prerequisite A.5/21 - - SUBSCRIBE response

Prerequisite: A.6/103 OR A.6/104 OR A.6/105 OR A.6/106 - - Additional for 3xx – 6xx response

**Table A.137A: Supported headers within the SUBSCRIBE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Error-Info | [26] 20.18 | o | o | [26] 20.18 | o | o |

Prerequisite A.5/21 - - SUBSCRIBE response

Prerequisite: A.6/103 OR A.6/35 - - Additional for 3xx or 485 (Ambiguous) response

**Table A.138: Supported headers within the SUBSCRIBE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Contact | [26] 20.10 | m (note) | m | [26] 20.10 | m | m |
| NOTE: | The strength of this requirement is RECOMMENDED rather than MANDATORY for a 485 response. | | | | | | |

Prerequisite A.5/21 - - SUBSCRIBE response

Prerequisite: A.6/14 - - Additional for 401 (Unauthorized) response

**Table A.139: Supported headers within the SUBSCRIBE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 2 | Proxy-Authenticate | [26] 20.27 | c1 | c1 | [26] 20.27 | c1 | c1 |
| 8 | WWW-Authenticate | [26] 20.44 | m | m | [26] 20.44 | m | m |
| c1: | IF A.5/7 THEN m ELSE n/a - - support of authentication between UA and UA. | | | | | | |

Prerequisite A.5/21 - - SUBSCRIBE response

Prerequisite: A.6/17 OR A.6/23 OR A.6/30 OR A.6/36 OR A.6/42 OR A.6/45 OR A.6/50 OR A.6/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480 (Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response

**Table A.140: Supported headers within the SUBSCRIBE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 3 | Retry-After | [26] 20.33 | o | | [26] 20.33 | o | |

**Table A.141: Void**

Prerequisite A.5/21 - - SUBSCRIBE response

Prerequisite: A.6/20 - - Additional for 407 (Proxy Authentication Required) response

**Table A.142: Supported headers within the SUBSCRIBE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 2 | Proxy-Authenticate | [26] 20.27 | c1 | c1 | [26] 20.27 | c1 | c1 |
| 6 | WWW-Authenticate | [26] 20.44 | o | o | [26] 20.44 | o | o |
| c1: | IF A.5/7 THEN m ELSE n/a - - support of authentication between UA and UA. | | | | | | |

Prerequisite A.5/21 - - SUBSCRIBE response

Prerequisite A.6/25 - - Additional for 415 (Unsupported Media Type) response

**Table A.143: Supported headers within the SUBSCRIBE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Accept | [26] 20.1 | o.1 | o.1 | [26] 20.1 | m | m |
| 2 | Accept-Encoding | [26] 20.2 | o.1 | o.1 | [26] 20.2 | m | m |
| 3 | Accept-Language | [26] 20.3 | o.1 | o.1 | [26] 20.3 | m | m |
| 6 | Server | [26] 20.35 | o | o | [26] 20.35 | o | o |
| o.1 | At least one of these capabilities is supported. | | | | | | |

Prerequisite A.5/21 - - SUBSCRIBE response

Prerequisite: A.6/27 - - Additional for 420 (Bad Extension) response

**Table A.144: Supported headers within the SUBSCRIBE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 5 | Unsupported | [26] 20.40 | m | m | [26] 20.40 | m | m |

Prerequisite A.5/21 - - SUBSCRIBE response

Prerequisite: A.6/28 OR A.6/41A - - Additional for 421 (Extension Required), 494 (Security Agreement Required) response

**Table A.144A: Supported headers within the SUBSCRIBE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 3 | Security-Server | [48] 2 | x | x | [48] 2 | c1 | c1 |
| c1: | IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. | | | | | | |

Prerequisite A.5/21 - - SUBSCRIBE response

Prerequisite: A.6/29 - - Additional for 423 (Interval Too Brief) response

**Table A.145: Supported headers within the SUBSCRIBE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 2 | Min-Expires | [26] 20.23 | m | m | [26] 20.23 | m | m |

**Table A.146: Void**

Prerequisite A.5/21 - - SUBSCRIBE response

Prerequisite: A.6/39 - - Additional for 489 (Bad Event) response

**Table A.147: Supported headers within the SUBSCRIBE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Allow-Events | [28] 7.2.2 | m | m | [28] 7.2.2 | m | m |

**Table A.148: Void**

Prerequisite A.5/21 - - SUBSCRIBE response

**Table A.149: Supported message bodies within the SUBSCRIBE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | | | | | | | |

### A.2.1.4.14 UPDATE method

Prerequisite A.5/22 - - UPDATE request

**Table A.150: Supported headers within the UPDATE request**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Accept | [26] 20.1 | o | o | [26] 20.1 | m | m |
| 1A | Accept-Contact | [56B] 9.2 | c20 | c20 | [56B] 9.2 | c24 | c24 |
| 2 | Accept-Encoding | [26] 20.2 | o | o | [26] 20.2 | m | m |
| 3 | Accept-Language | [26] 20.3 | o | o | [26] 20.3 | m | m |
| 4 | Allow | [26] 20.5 | o | o | [26] 20.5 | m | m |
| 5 | Allow-Events | [28] 7.2.2 | c2 | c2 | [28] 7.2.2 | c3 | c3 |
| 6 | Authorization | [26] 20.7 | c4 | c4 | [26] 20.7 | c4 | c4 |
| 7 | Call-ID | [26] 20.8 | m | m | [26] 20.8 | m | m |
| 8 | Call-Info | [26] 20.9 | o | o | [26] 20.9 | o | o |
| 9 | Contact | [26] 20.10 | m | m | [26] 20.10 | m | m |
| 10 | Content-Disposition | [26] 20.11 | o | o | [26] 20.11 | m | m |
| 11 | Content-Encoding | [26] 20.12 | o | o | [26] 20.12 | m | m |
| 12 | Content-Language | [26] 20.13 | o | o | [26] 20.13 | m | m |
| 13 | Content-Length | [26] 20.14 | m | m | [26] 20.14 | m | m |
| 14 | Content-Type | [26] 20.15 | m | m | [26] 20.15 | m | m |
| 15 | Cseq | [26] 20.16 | m | m | [26] 20.16 | m | m |
| 16 | Date | [26] 20.17 | c5 | c5 | [26] 20.17 | m | m |
| 17 | From | [26] 20.20 | m | m | [26] 20.20 | m | m |
| 18 | Max-Forwards | [26] 20.22 | m | m | [26] 20.22 | n/a | n/a |
| 19 | MIME-Version | [26] 20.24 | o | o | [26] 20.24 | m | m |
| 19A | Min-SE | [58] 5 | c21 | c21 | [58] 5 | c21 | c21 |
| 20 | Organization | [26] 20.25 | o | o | [26] 20.25 | o | o |
| 20A | P-Access-Network-Info | [52] 4.4 | c11 | c12 | [52] 4.4 | c11 | c13 |
| 20B | P-Charging-Function-Addresses | [52] 4.5 | c16 | c17 | [52] 4.5 | c16 | c17 |
| 20C | P-Charging-Vector | [52] 4.6 | c14 | c15 | [52] 4.6 | c14 | c15 |
| 20D | Privacy | [33] 4.2 | c6 | n/a | [33] 4.2 | c6 | n/a |
| 21 | Proxy-Authorization | [26] 20.28 | c10 | c10 | [26] 20.28 | n/a | n/a |
| 22 | Proxy-Require | [26] 20.29 | o | n/a | [26] 20.29 | n/a | n/a |
| 22A | Reason | [34A] 2 | c8 | c8 | [34A] 2 | c8 | c8 |
| 23 | Record-Route | [26] 20.30 | n/a | n/a | [26] 20.30 | n/a | n/a |
| 23A | Referred-By | [59] 3 | c22 | c22 | [59] 3 | c23 | c23 |
| 23B | Reject-Contact | [56B] 9.2 | c20 | c20 | [56B] 9.2 | c24 | c24 |
| 23C | Request-Disposition | [56B] 9.1 | c20 | c20 | [56B] 9.1 | c24 | c24 |
| 24 | Require | [26] 20.32 | o | o | [26] 20.32 | m | m |
| 25 | Route | [26] 20.34 | m | m | [26] 20.34 | n/a | n/a |
| 25A | Security-Client | [48] 2.3.1 | c18 | c18 | [48] 2.3.1 | n/a | n/a |
| 25B | Security-Verify | [48] 2.3.1 | c19 | c19 | [48] 2.3.1 | n/a | n/a |
| 25C | Session-Expires | [58] 4 | c21 | c21 | [58] 4 | c21 | c21 |
| 26 | Supported | [26] 20.37 | o | o | [26] 20.37 | m | m |
| 27 | Timestamp | [26] 20.38 | c9 | c9 | [26] 20.38 | m | m |
| 28 | To | [26] 20.39 | m | m | [26] 20.39 | m | m |
| 29 | User-Agent | [26] 20.41 | o | o | [26] 20.41 | o | o |
| 30 | Via | [26] 20.42 | m | m | [26] 20.42 | m | m |

| | |
|---|---|
| c2: | IF A.4/20 THEN o ELSE n/a - - SIP specific event notification extension. |
| c3: | IF A.4/20 THEN m ELSE n/a - - SIP specific event notification extension. |
| c4: | IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA. |
| c5: | IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses. |
| c6: | IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP). |
| c8: | IF A.4/38 THEN o ELSE n/a - - the Reason header field for the session initiation protocol. |
| c9: | IF A.4/6 THEN o ELSE n/a - - timestamping of requests. |
| c10: | IF A.4/8A THEN m ELSE n/a - - authentication between UA and proxy. |
| c11: | IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension. |
| c12: | IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE. |
| c13: | IF A.4/34 AND (A.3/7A OR A.3/7D) THEN m ELSE n/a - - the P-Access-Network-Info header extension and AS acting as terminating UA or AS acting as third-party call controller. |
| c14: | IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension. |
| c15: | IF A.4/36 THEN m ELSE n/a - - the P-Charging-Vector header extension. |
| c16: | IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension. |
| c17: | IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension. |
| c18: | IF A.4/37 THEN o ELSE n/a - - security mechanism agreement for the session initiation protocol (note). |
| c19: | IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. |
| c20: | IF A.4/40 THEN o ELSE n/a - - caller preferences for the session initiation protocol. |
| c21: | IF A.4/42 THEN m ELSE n/a - - the SIP session timer. |
| c22: | IF A.4/43 THEN m ELSE n/a - - the SIP Referred-By mechanism. |
| c23: | IF A.4/43 THEN o ELSE n/a - - the SIP Referred-By mechanism. |
| c24: | IF A.4/40 THEN m ELSE n/a - - caller preferences for the session initiation protocol. |
| NOTE: | Support of this header in this method is dependent on the security mechanism and the security architecture which is implemented. Use of this header in this method is not appropriate to the security mechanism defined by 3GPP TS 33.203 [19]. |

Prerequisite A.5/22 - - UPDATE request

**Table A.151: Supported message bodies within the UPDATE request**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | | | | | | | |

Prerequisite A.5/23 - - UPDATE response for all status-codes

**Table A.152: Supported headers within the UPDATE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 0A | Allow | [26] 20.5 | c11 | c11 | [26] 20.5 | m | m |
| 1 | Call-ID | [26] 20.8 | m | m | [26] 20.8 | m | m |
| 1A | Call-Info | [26] 20.9 | o | o | [26] 20.9 | o | o |
| 1B | Contact | [26] 20.10 | o | o | [26] 20.10 | o | o |
| 2 | Content-Disposition | [26] 20.11 | o | o | [26] 20.11 | m | m |
| 3 | Content-Encoding | [26] 20.12 | o | o | [26] 20.12 | m | m |
| 4 | Content-Language | [26] 20.13 | o | o | [26] 20.13 | m | m |
| 5 | Content-Length | [26] 20.14 | m | m | [26] 20.14 | m | m |
| 6 | Content-Type | [26] 20.15 | m | m | [26] 20.15 | m | m |
| 7 | Cseq | [26] 20.16 | m | m | [26] 20.16 | m | m |
| 8 | Date | [26] 20.17 | c1 | c1 | [26] 20.17 | m | m |
| 9 | From | [26] 20.20 | m | m | [26] 20.20 | m | m |
| 10 | MIME-Version | [26] 20.24 | o | o | [26] 20.24 | m | m |
| 10A | Organization | [26] 20.25 | o | o | [26] 20.25 | o | o |
| 10B | P-Access-Network-Info | [52] 4.4 | c4 | c5 | [52] 4.4 | c4 | c6 |
| 10C | P-Charging-Function-Addresses | [52] 4.5 | c9 | c10 | [52] 4.5 | c9 | c10 |
| 10D | P-Charging-Vector | [52] 4.6 | c7 | c8 | [52] 4.6 | c7 | c8 |
| 10E | Privacy | [33] 4.2 | c3 | n/a | [33] 4.2 | c3 | n/a |
| 10F | Require | [26] 20.31 | m | m | [26] 20.31 | m | m |
| 10G | Server | [26] 20.35 | o | o | [26] 20.35 | o | o |
| 11 | Timestamp | [26] 20.38 | c12 | c12 | [26] 20.38 | c2 | c2 |
| 12 | To | [26] 20.39 | m | m | [26] 20.39 | m | m |
| 12A | User-Agent | [26] 20.41 | o | o | [26] 20.41 | o | o |
| 13 | Via | [26] 20.42 | m | m | [26] 20.42 | m | m |
| 14 | Warning | [26] 20.43 | o (note) | o | [26] 20.43 | o | o |
| c1: | IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses. | | | | | | |
| c2: | IF A.4/6 THEN m ELSE n/a - - timestamping of requests. | | | | | | |
| c3: | IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP). | | | | | | |
| c4: | IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension. | | | | | | |
| c5: | IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE. | | | | | | |
| c6: | IF A.4/34 AND (A.3/7A OR A.3/7D) THEN m ELSE n/a - - the P-Access-Network-Info header extension and AS acting as terminating UA or AS acting as third-party call controller. | | | | | | |
| c7: | IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension. | | | | | | |
| c8: | IF A.4/36 THEN m ELSE n/a - - the P-Charging-Vector header extension. | | | | | | |
| c9: | IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension. | | | | | | |
| c10: | IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension. | | | | | | |
| c11: | IF A.6/18 THEN m ELSE o - - 405 (Method Not Allowed) | | | | | | |
| c12: | IF A.4/6 THEN o ELSE n/a - - timestamping of requests. | | | | | | |
| NOTE: | For a 488 (Not Acceptable Here) response, RFC 3261 [26] gives the status of this header as SHOULD rather than OPTIONAL. | | | | | | |

Prerequisite A.5/23 - - UPDATE response

Prerequisite: A.6/102 - - Additional for 2xx response

**Table A.153: Supported headers within the UPDATE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 0A | Accept | [26] 20.1 | o | o | [26] 20.1 | m | m |
| 0B | Accept-Encoding | [26] 20.2 | o | o | [26] 20.2 | m | m |
| 0C | Accept-Language | [26] 20.3 | o | o | [26] 20.3 | m | m |
| 1 | Allow-Events | [28] 7.2.2 | c4 | c4 | [28] 7.2.2 | c5 | c5 |
| 2 | Authentication-Info | [26] 20.6 | c1 | c1 | [26] 20.6 | c2 | c2 |
| 3 | Contact | [26] 20.10 | m | m | [26] 20.10 | m | m |
| 4 | Session-Expires | [58] | c3 | c3 | [58] | c3 | c3 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 6 | Supported | [26] 20.37 | m | m | [26] 20.37 | m | m |
| c1: | IF A.4/7 THEN o ELSE n/a - - authentication between UA and UA. | | | | | | |
| c2: | IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA. | | | | | | |
| c3: | IF A.4/42 THEN m ELSE n/a - - the SIP session timer | | | | | | |
| c4: | IF A.4/20 THEN o ELSE n/a - - SIP specific event notification extension. | | | | | | |
| c5: | IF A.4/20 THEN m ELSE n/a - - SIP specific event notification extension. | | | | | | |

Prerequisite A.5/23 - - UPDATE response

Prerequisite: A.6/103 OR A.6/104 OR A.6/105 OR A.6/106 - - Additional for 3xx – 6xx response

**Table A.153A: Supported headers within the UPDATE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Error-Info | [26] 20.18 | o | o | [26] 20.18 | o | o |

Prerequisite A.5/23 - - UPDATE response

Prerequisite: A.6/103 OR A.6/35 - - Additional for 3xx, 485 (Ambiguous) response

**Table A.154: Supported headers within the UPDATE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 2 | Contact | [26] 20.10 | o | o | [26] 20.10 | o | o |

Prerequisite A.5/23 - - UPDATE response

Prerequisite: A.6/14 - - Additional for 401 (Unauthorized) response

**Table A.154A: Supported headers within the UPDATE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 3 | Proxy-Authenticate | [26] 20.27 | o | | [26] 20.27 | o | |
| 6 | WWW-Authenticate | [26] 20.44 | m | m | [26] 20.44 | m | m |
| c1: | IF A.5/7 THEN m ELSE n/a - - support of authentication between UA and UA. | | | | | | |

Prerequisite A.5/23 - - UPDATE response

Prerequisite: A.6/17 OR A.6/23 OR A.6/30 OR A.6/36 OR A.6/42 OR A.6/45 OR A.6/50 OR A.6/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response

**Table A.155: Supported headers within the UPDATE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 5 | Retry-After | [26] 20.33 | o | o | [26] 20.33 | o | o |

**Table A.156: Void**

Prerequisite A.5/23 - - UPDATE response

Prerequisite: A.6/20 - - Additional for 407 (Proxy Authentication Required) response

**Table A.157: Supported headers within the UPDATE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 4 | Proxy-Authenticate | [26] 20.27 | c1 | c1 | [26] 20.27 | c1 | c1 |
| 8 | WWW-Authenticate | [26] 20.44 | o | o | [26] 20.44 | o | o |
| c1: | IF A.5/7 THEN m ELSE n/a - - support of authentication between UA and UA. | | | | | | |

Prerequisite A.5/23 - - UPDATE response

Prerequisite: A.6/25 - - Additional for 415 (Unsupported Media Type) response

**Table A.158: Supported headers within the UPDATE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Accept | [26] 20.1 | o.1 | o.1 | [26] 20.1 | m | m |
| 2 | Accept-Encoding | [26] 20.2 | o.1 | o.1 | [26] 20.2 | m | m |
| 3 | Accept-Language | [26] 20.3 | o.1 | o.1 | [26] 20.3 | m | m |
| o.1 | At least one of these capabilities is supported. | | | | | | |

Prerequisite A.5/23 - - UPDATE response

Prerequisite: A.6/27 - - Additional for 420 (Bad Extension) response

**Table A.159: Supported headers within the UPDATE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 7 | Unsupported | [26] 20.40 | m | m | [26] 20.40 | m | m |

Prerequisite A.5/23 - - UPDATE response

Prerequisite: A.6/28 OR A.6/41A - - Additional for 421 (Extension Required), 494 (Security Agreement Required) response

**Table A.159A: Supported headers within the UPDATE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 3 | Security-Server | [48] 2 | x | x | [48] 2 | c1 | c1 |
| c1: | IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. | | | | | | |

Prerequisite A.5/23 - - UPDATE response

Prerequisite: A.6/28A - - Additional for 422 (Session Interval Too Small) response

**Table A.159B: Supported headers within the UPDATE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Min-SE | [58] 5 | c1 | c1 | [58] 5 | c1 | c1 |
| c1: | IF A.4/42 THEN m ELSE n/a - - the SIP session timer. | | | | | | |

**Table A.160: Void**

Prerequisite A.5/23 - - UPDATE response

**Table A.161: Supported message bodies within the UPDATE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | | | | | | | |

# A.2.2 Proxy role

## A.2.2.1 Introduction

This subclause contains the ICS proforma tables related to the proxy role. They need to be completed only for proxy implementations.

Prerequisite: A.2/2 - - proxy role

### A.2.2.2 Major capabilities

**Table A.162: Major capabilities**

| Item | Does the implementation support | Reference | RFC status | Profile status |
|---|---|---|---|---|
| | **Capabilities within main protocol** | | | |
| 3 | initiate session release? | [26] 16 | x | c27 |
| 4 | stateless proxy behaviour? | [26] 16.11 | o.1 | c28 |
| 5 | stateful proxy behaviour? | [26] 16.2 | o.1 | c29 |
| 6 | forking of initial requests? | [26] 16.1 | c1 | c31 |
| 7 | support of indication of TLS connections in the Record-Route header on the upstream side? | [26] 16.7 | o | n/a |
| 8 | support of indication TLS connections in the Record-Route header on the downstream side? | [26] 16.7 | o | n/a |
| 8A | authentication between UA and proxy? | [26] 20.28, 22.3 | o | x |
| 9 | insertion of date in requests and responses? | [26] 20.17 | o | o |
| 10 | suppression or modification of alerting information data? | [26] 20.4 | o | o |
| 11 | reading the contents of the Require header before proxying the request or response? | [26] 20.32 | o | o |
| 12 | adding or modifying the contents of the Require header before proxying the REGISTER request or response | [26] 20.32 | o | m |
| 13 | adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER? | [26] 20.32 | o | o |
| 14 | being able to insert itself in the subsequent transactions in a dialog (record-routing)? | [26] 16.6 | o | c2 |
| 15 | the requirement to be able to use separate URIs in the upstream direction and downstream direction when record routeing? | [26] 16.7 | c3 | c3 |
| 16 | reading the contents of the Supported header before proxying the response? | [26] 20.37 | o | o |
| 17 | reading the contents of the Unsupported header before proxying the 420 response to a REGISTER? | [26] 20.40 | o | m |
| 18 | reading the contents of the Unsupported header before proxying the 420 response to a method other than REGISTER? | [26] 20.40 | o | o |
| 19 | the inclusion of the Error-Info header in 3xx - 6xx responses? | [26] 20.18 | o | o |
| 19A | reading the contents of the Organization header before proxying the request or response? | [26] 20.25 | o | o |
| 19B | adding or concatenating the Organization header before proxying the request or response? | [26] 20.25 | o | o |
| 19C | reading the contents of the Call-Info header before proxying the request or response? | [26] 20.25 | o | o |
| 19D | adding or concatenating the Call-Info header before proxying the request or response? | [26] 20.25 | o | o |
| 19E | delete Contact headers from 3xx responses prior to relaying the response? | [26] 20 | o | o |
| | **Extensions** | | | |

| | | | | |
|---|---|---|---|---|
| 20 | the SIP INFO method? | [25] | o | o |
| 21 | reliability of provisional responses in SIP? | [27] | o | i |
| 22 | the REFER method? | [36] | o | o |
| 23 | integration of resource management and SIP? | [30] [64] | o | i |
| 24 | the SIP UPDATE method? | [29] | c4 | i |
| 26 | SIP extensions for media authorization? | [31] | o | c7 |
| 27 | SIP specific event notification | [28] | o | i |
| 28 | the use of NOTIFY to establish a dialog | [28] 4.2 | o | n/a |
| 29 | Session Initiation Protocol Extension Header Field for Registering Non-Adjacent Contacts | [35] | o | c6 |
| 30 | extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks | [34] | o | m |
| 30A | act as first entity within the trust domain for asserted identity | [34] | c5 | c8 |
| 30B | act as subsequent entity within trust network that can route outside the trust network | [34] | c5 | c9 |
| 31 | a privacy mechanism for the Session Initiation Protocol (SIP) | [33] | o | m |
| 31A | request of privacy by the inclusion of a Privacy header | [33] | n/a | n/a |
| 31B | application of privacy based on the received Privacy header | [33] | c10 | c12 |
| 31C | passing on of the Privacy header transparently | [33] | c10 | c13 |
| 31D | application of the privacy option "header" such that those headers which cannot be completely expunged of identifying information without the assistance of intermediaries are obscured? | [33] 5.1 | x | x |
| 31E | application of the privacy option "session" such that anonymization for the session(s) initiated by this message occurs? | [33] 5.2 | n/a | n/a |
| 31F | application of the privacy option "user" such that user level privacy functions are provided by the network? | [33] 5.3 | n/a | n/a |
| 31G | application of the privacy option "id" such that privacy of the network asserted identity is provided by the network? | [34] 7 | c11 | c12 |
| 32 | Session Initiation Protocol Extension Header Field for Service Route Discovery During Registration | [38] | o | c30 |
| 33 | a messaging mechanism for the Session Initiation Protocol (SIP) | [50] | o | m |
| 34 | Compressing the Session Initiation Protocol | [55] | o | c7 |
| 35 | private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP)? | [52] | o | m |
| 36 | the P-Associated-URI header extension? | [52] 4.1 | c14 | c15 |
| 37 | the P-Called-Party-ID header extension? | [52] 4.2 | c14 | c16 |
| 38 | the P-Visited-Network-ID header extension? | [52] 4.3 | c14 | c17 |
| 39 | reading, or deleting the P-Visited-Network-ID header before proxying the request or response? | [52] 4.3 | c18 | n/a |
| 41 | the P-Access-Network-Info header | [52] 4.4 | c14 | c19 |

| | | | | |
|---|---|---|---|---|
| | extension? | | | |
| 42 | act as first entity within the trust domain for access network information? | [52] 4.4 | c20 | c21 |
| 43 | act as subsequent entity within trust network for access network information that can route outside the trust network? | [52] 4.4 | c20 | c22 |
| 44 | the P-Charging-Function-Addresses header extension? | [52] 4.5 | c14 | m |
| 44A | adding, deleting or reading the P-Charging-Function-Addresses header before proxying the request or response? | [52] 4.6 | c25 | c26 |
| 45 | the P-Charging-Vector header extension? | [52] 4.6 | c14 | m |
| 46 | adding, deleting, reading or modifying the P-Charging-Vector header before proxying the request or response? | [52] 4.6 | c23 | c24 |
| 47 | security mechanism agreement for the session initiation protocol? | [48] | o | c7 |
| 48 | the Reason header field for the session initiation protocol | [34A] | o | o |
| 49 | an extension to the session initiation protocol for symmetric response routeing | [56A] | o | x |
| 50 | caller preferences for the session initiation protocol? | [56B] | c33 | c33 |
| 50A | the proxy-directive within caller-preferences? | [56B] 9.1 | o.4 | o.4 |
| 50B | the cancel-directive within caller-preferences? | [56B] 9.1 | o.4 | o.4 |
| 50C | the fork-directive within caller-preferences? | [56B] 9.1 | o.4 | c32 |
| 50D | the recurse-directive within caller-preferences? | [56B] 9.1 | o.4 | o.4 |
| 50E | the parallel-directive within caller-preferences? | [56B] 9.1 | o.4 | c32 |
| 50F | the queue-directive within caller-preferences? | [56B] 9.1 | o.4 | o.4 |
| 51 | an event state publication extension to the session initiation protocol? | [70] | o | m |
| 52 | SIP session timer? | [58] | o | o |
| 53 | the SIP Referred-By mechanism? | [59] | o | o |
| 54 | the Session Inititation Protocol (SIP) "Replaces" header? | [60] | o | o |
| 55 | the Session Inititation Protocol (SIP) "Join" header? | [61] | o | o |
| 56 | the callee capabillities? | [62] | o | o |

| | |
|---|---|
| c1: | IF A.162/5 THEN o ELSE n/a - - stateful proxy behaviour. |
| c2: | IF A.3/2 OR A.3/3A OR A.3/4 THEN m ELSE o - - P-CSCF, I-CSCF(THIG) or S-CSCF. |
| c3: | IF (A.162/7 AND NOT A.162/8) OR (NOT A.162/7 AND A.162/8) THEN m ELSE IF A.162/14 THEN o ELSE n/a - - TLS interworking with non-TLS else proxy insertion. |
| c4: | IF A.162/23 THEN m ELSE o - - integration of resource management and SIP. |
| c5: | IF A.162/30 THEN o ELSE n/a - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks. |
| c6: | IF A.3/2 OR A.3/3A THEN m ELSE n/a - - P-CSCF or I-CSCF (THIG). |
| c7: | IF A.3/2 THEN m ELSE n/a - - P-CSCF. |
| c8: | IF A.3/2 AND A.162/30 THEN m ELSE n/a - - P-CSCF and extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks. |
| c9: | IF A.3/2 AND A.162/30 THEN m ELSE IF A.3/7C AND A.162/30 THEN o ELSE n/a - - S-CSCF or AS acting as proxy and extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks (NOTE). |
| c10: | IF A.162/31 THEN o.2 ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP). |
| c11: | IF A.162/31B THEN o ELSE x - - application of privacy based on the received Privacy header. |
| c12: | IF A.162/31 AND A.3/4 THEN m ELSE n/a - - S-CSCF. |
| c13: | IF A.162/31 AND (A.3/2 OR A.3/3 OR A.3/7C) THEN m ELSE n/a - - P-CSCF OR I-CSCF OR AS acting as a SIP proxy. |
| c14: | IF A.162/35 THEN o.3 ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP). |
| c15: | IF A.162/35 AND (A.3/2 OR A.3/3) THEN m THEN o ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and P-CSCF or I-CSCF. |
| c16: | IF A.162/35 AND (A.3/2 OR A.3/3 OR A.3/4) THEN m ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and P-CSCF or I-CSCF or S-CSCF. |
| c17: | IF A.162/35 AND (A.3/2 OR A.3/3) THEN m ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and P-CSCF or I-CSCF. |
| c18: | IF A.162/38 THEN o ELSE n/a - - the P-Visited-Network-ID header extension. |
| c19: | IF A.162/35 AND (A.3/2 OR A.3.3 OR A.3/4 OR A.3/7 THEN m ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and P-CSCF, I-CSCF, S-CSCF, AS acting as a proxy. |
| c20: | IF A.162/41 THEN o ELSE n/a - - the P-Access-Network-Info header extension. |
| c21: | IF A.162/41 AND A.3/2 THEN m ELSE n/a - - the P-Access-Network-Info header extension and P-CSCF. |
| c22: | IF A.162/41 AND A.3/4 THEN m ELSE n/a - - the P-Access-Network-Info header extension and S-CSCF. |
| c23: | IF A.162/45 THEN o ELSE n/a - - the P-Charging-Vector header extension. |
| c24: | IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension. |
| c25: | IF A.162/44 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension. |
| c26: | IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function Addresses header extension. |
| c27: | IF A.3/2 OR A.3/4 THEN m ELSE x - - P-CSCF or S-CSCF. |
| c28: | IF A.3/2 OR A.3/4 OR A.3/6 then m ELSE o - - P-CSCF or S-CSCF of MGCF. |
| c29: | IF A.3/2 OR A.3/4 OR A.3/6 then o ELSE m - - P-CSCF or S-CSCF of MGCF. |
| c30: | IF A.3/2 o ELSE i - - P-CSCF. |
| c31: | IF A.3/4 THEN m ELSE x - - S-CSCF. |
| c32: | IF A.3/4 THEN m ELSE o.4 - - S-CSCF. |
| c33: | IF A.162/50A OR A.162/50B OR A.162/50C OR A.162/50D OR A.162/50E OR A.162/50F THEN m ELSE n/a - - support of any directives within caller preferences for the session initiation protocol. |
| o.1: | It is mandatory to support at least one of these items. |
| o.2: | It is mandatory to support at least one of these items. |
| o.3: | It is mandatory to support at least one of these items. |
| o.4 | At least one of these capabilities is supported. |
| NOTE: | An AS acting as a proxy may be outside the trust domain, and therefore not able to support the capability for that reason; in this case it is perfectly reasonable for the header to be passed on transparently, as specified in the PDU parts of the profile. |

### A.2.2.3 PDUs

**Table A.163: Supported methods**

| Item | PDU | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | ACK request | [26] 13 | m | m | [26] 13 | m | m |
| 2 | BYE request | [26] 16 | m | m | [26] 16 | m | m |
| 3 | BYE response | [26] 16 | m | m | [26] 16 | m | m |
| 4 | CANCEL request | [26] 16.10 | m | m | [26] 16.10 | m | m |
| 5 | CANCEL response | [26] 16.10 | m | m | [26] 16.10 | m | m |
| 8 | INVITE request | [26] 16 | m | m | [26] 16 | m | m |
| 9 | INVITE response | [26] 16 | m | m | [26] 16 | m | m |
| 9A | MESSAGE request | [50] 4 | c5 | c5 | [50] 7 | c5 | c5 |
| 9B | MESSAGE response | [50] 4 | c5 | c5 | [50] 7 | c5 | c5 |
| 10 | NOTIFY request | [28] 8.1.2 | c3 | c3 | [28] 8.1.2 | c3 | c3 |
| 11 | NOTIFY response | [28] 8.1.2 | c3 | c3 | [28] 8.1.2 | c3 | c3 |
| 12 | OPTIONS request | [26] 16 | m | m | [26] 16 | m | m |
| 13 | OPTIONS response | [26] 16 | m | m | [26] 16 | m | m |
| 14 | PRACK request | [27] 6 | c6 | c6 | [27] 6 | c6 | c6 |
| 15 | PRACK response | [27] 6 | c6 | c6 | [27] 6 | c6 | c6 |
| 15A | PUBLISH request | [70] 11.1.1 | c20 | c20 | [70] 11.1.1 | c20 | c20 |
| 15B | PUBLISH response | [70] 11.1.1 | c20 | c20 | [70] 11.1.1 | c20 | c20 |
| 16 | REFER request | [36] 3 | c1 | c1 | [36] 3 | c1 | c1 |
| 17 | REFER response | [36] 3 | c1 | c1 | [36] 3 | c1 | c1 |
| 18 | REGISTER request | [26] 16 | m | m | [26] 16 | m | m |
| 19 | REGISTER response | [26] 16 | m | m | [26] 16 | m | m |
| 20 | SUBSCRIBE request | [28] 8.1.1 | c3 | c3 | [28] 8.1.1 | c3 | c3 |
| 21 | SUBSCRIBE response | [28] 8.1.1 | c3 | c3 | [28] 8.1.1 | c3 | c3 |
| 22 | UPDATE request | [29] 7 | c4 | c4 | [29] 7 | c4 | c4 |
| 23 | UPDATE response | [29] 7 | c4 | c4 | [29] 7 | c4 | c4 |
| c1: | IF A.162/22 THEN m ELSE n/a - - the REFER method. | | | | | | |
| c3 | IF A.162/27 THEN m ELSE n/a - - SIP specific event notification. | | | | | | |
| c4 | IF A.162/24 THEN m ELSE n/a - - the SIP UPDATE method. | | | | | | |
| c5: | IF A.162/33 THEN m ELSE n/a - - the SIP MESSAGE method. | | | | | | |
| c6: | ÌF A.162/21 THEN m ELSE n/a - - reliability of provisional responses. | | | | | | |
| c20: | IF A.4/51 THEN m ELSE n/a | | | | | | |

## A.2.2.4 PDU parameters

### A.2.2.4.1 Status-codes

**Table A.164: Supported-status codes**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | 100 (Trying) | [26] 21.1.1 | c1 | c1 | [26] 21.1.1 | c2 | c2 |
| 101 | 1xx response | [26] 21.1 | p21 | p21 | [26] 21.1 | p21 | p21 |
| 2 | 180 (Ringing) | [26] 21.1.2 | c3 | c3 | [26] 21.1.2 | c3 | c3 |
| 3 | 181 (Call Is Being Forwarded) | [26] 21.1.3 | c3 | c3 | [26] 21.1.3 | c3 | c3 |
| 4 | 182 (Queued) | [26] 21.1.4 | c3 | c3 | [26] 21.1.4 | c3 | c3 |
| 5 | 183 (Session Progress) | [26] 21.1.5 | c3 | c3 | [26] 21.1.5 | c3 | c3 |
| 102 | 2xx response | [26] 21.2 | p22 | p22 | [26] 21.1 | p22 | p22 |
| 6 | 200 (OK) | [26] 21.2.1 | m | m | [26] 21.2.1 | i | m |
| 7 | 202 (Accepted) | [28] 8.3.1 | c4 | c4 | [28] 8.3.1 | c4 | c4 |
| 103 | 3xx response | [26] 21.3 | p23 | p23 | [26] 21.1 | p23 | p23 |
| 8 | 300 (Multiple Choices) | [26] 21.3.1 | m | m | [26] 21.3.1 | i | i |
| 9 | 301 (Moved Permanently) | [26] 21.3.2 | m | m | [26] 21.3.2 | i | i |
| 10 | 302 (Moved Temporarily) | [26] 21.3.3 | m | m | [26] 21.3.3 | i | i |
| 11 | 305 (Use Proxy) | [26] 21.3.4 | m | m | [26] 21.3.4 | i | i |
| 12 | 380 (Alternative Service) | [26] 21.3.5 | m | m | [26] 21.3.5 | i | i |
| 104 | 4xx response | [26] 21.4 | p24 | p24 | [26] 21.4 | p24 | p24 |
| 13 | 400 (Bad Request) | [26] 21.4.1 | m | m | [26] 21.4.1 | i | i |
| 14 | 401 (Unauthorized) | [26] 21.4.2 | m | m | [26] 21.4.2 | i | c10 |
| 15 | 402 (Payment Required) | [26] 21.4.3 | n/a | n/a | [26] 21.4.3 | n/a | n/a |
| 16 | 403 (Forbidden) | [26] 21.4.4 | m | m | [26] 21.4.4 | i | i |
| 17 | 404 (Not Found) | [26] 21.4.5 | m | m | [26] 21.4.5 | i | i |
| 18 | 405 (Method Not Allowed) | [26] 21.4.6 | m | m | [26] 21.4.6 | i | i |
| 19 | 406 (Not Acceptable) | [26] 21.4.7 | m | m | [26] 21.4.7 | i | i |
| 20 | 407 (Proxy Authentication Required) | [26] 21.4.8 | m | m | [26] 21.4.8 | i | i |
| 21 | 408 (Request Timeout) | [26] 21.4.9 | m | m | [26] 21.4.9 | i | i |
| 22 | 410 (Gone) | [26] 21.4.10 | m | m | [26] 21.4.10 | i | i |
| 22A | 412 (Conditional Request Failed) | [70] 11.2.1 | c20 | c20 | [70] 11.2.1 | c19 | c19 |
| 23 | 413 (Request Entity Too Large) | [26] 21.4.11 | m | m | [26] 21.4.11 | i | i |
| 24 | 414 (Request-URI Too Large) | [26] 21.4.12 | m | m | [26] 21.4.12 | i | i |
| 25 | 415 (Unsupported Media Type) | [26] 21.4.13 | m | m | [26] 21.4.13 | i | i |
| 26 | 416 (Unsupported URI | [26] | m | m | [26] | i | i |

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| | Scheme) | 21.4.14 | | | 21.4.14 | | |
| 27 | 420 (Bad Extension) | [26] 21.4.15 | m | m | [26] 21.4.15 | i | i |
| 28 | 421 (Extension Required) | [26] 21.4.16 | m | m | [26] 21.4.16 | i | i |
| 28A | 422 (Session Interval Too Small) | [58] 6 | c8 | c8 | [58] 6 | c8 | c8 |
| 29 | 423 (Interval Too Brief) | [26] 21.4.17 | c5 | c5 | [26] 21.4.17 | c6 | c6 |
| 29A | 429 (Provide Referrer Identity) | [59] 5 | c9 | c9 | [59] 5 | c9 | c9 |
| 30 | 480 (Temporarily not available) | [26] 21.4.18 | m | m | [26] 21.4.18 | i | i |
| 31 | 481 (Call /Transaction Does Not Exist) | [26] 21.4.19 | m | m | [26] 21.4.19 | i | i |
| 32 | 482 (Loop Detected) | [26] 21.4.20 | m | m | [26] 21.4.20 | i | i |
| 33 | 483 (Too Many Hops) | [26] 21.4.21 | m | m | [26] 21.4.21 | i | i |
| 34 | 484 (Address Incomplete) | [26] 21.4.22 | m | m | [26] 21.4.22 | i | i |
| 35 | 485 (Ambiguous) | [26] 21.4.23 | m | m | [26] 21.4.23 | i | i |
| 36 | 486 (Busy Here) | [26] 21.4.24 | m | m | [26] 21.4.24 | i | i |
| 37 | 487 (Request Terminated) | [26] 21.4.25 | m | m | [26] 21.4.25 | i | i |
| 38 | 488 (Not Acceptable Here) | [26] 21.4.26 | m | m | [26] 21.4.26 | i | i |
| 39 | 489 (Bad Event) | [28] 7.3.2 | c4 | c4 | [28] 7.3.2 | c4 | c4 |
| 40 | 491 (Request Pending) | [26] 21.4.27 | m | m | [26] 21.4.27 | i | i |
| 41 | 493 (Undecipherable) | [26] 21.4.28 | m | m | [26] 21.4.28 | i | i |
| 41A | 494 (Security Agreement Required) | [48] 2 | c7 | c7 | [48] 2 | n/a | n/a |
| 105 | 5xx response | [26] 21.5 | p25 | p25 | [26] 21.5 | p25 | p25 |
| 42 | 500 (Internal Server Error) | [26] 21.5.1 | m | m | [26] 21.5.1 | i | i |
| 43 | 501 (Not Implemented) | [26] 21.5.2 | m | m | [26] 21.5.2 | i | i |
| 44 | 502 (Bad Gateway) | [26] 21.5.3 | m | m | [26] 21.5.3 | i | i |
| 45 | 503 (Service Unavailable) | [26] 21.5.4 | m | m | [26] 21.5.4 | i | i |
| 46 | 504 (Server Time-out) | [26] 21.5.5 | m | m | [26] 21.5.5 | i | i |
| 47 | 505 (Version not supported) | [26] 21.5.6 | m | m | [26] 21.5.6 | i | i |
| 48 | 513 (Message Too Large) | [26] 21.5.7 | m | m | [26] 21.5.7 | i | i |
| 49 | 580 (Precondition Failure) | [30] 8 | m | m | [30] 8 | i | i |
| 106 | 6xx response | [26] 21.6 | p26 | p26 | [26] 21.6 | p26 | p26 |
| 50 | 600 (Busy Everywhere) | [26] 21.6.1 | m | m | [26] 21.6.1 | i | i |
| 51 | 603 (Decline) | [26] 21.6.2 | m | m | [26] 21.6.2 | i | i |
| 52 | 604 (Does Not Exist Anywhere) | [26] 21.6.3 | m | m | [26] 21.6.3 | i | i |
| 53 | 606 (Not Acceptable) | [26] 21.6.4 | m | m | [26] 21.6.4 | i | i |

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| c1: | IF A.163/9 AND A.162/5 THEN m ELSE n/a - - INVITE response, stateful proxy. | | | | | | |
| c2: | IF A.163/9 THEN (IF A.162/5 THEN m ELSE i) ELSE n/a - - INVITE response, stateful proxy. | | | | | | |
| c3: | IF A.163/9 THEN m ELSE n/a - - INVITE response. | | | | | | |
| c4: | IF A.162/27 THEN m ELSE n/a - - SIP specific event notification. | | | | | | |
| c5: | IF A.163/19 OR A.163/21 THEN m ELSE n/a - - REGISTER response or SUBSCRIBE response. | | | | | | |
| c6: | IF A.163/19 OR A.163/21 THEN i ELSE n/a - - REGISTER response or SUBSCRIBE response. | | | | | | |
| c7: | IF A.162/47 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. | | | | | | |
| c8: | IF A.162/52 THEN m ELSE n/a - - the SIP session timer. | | | | | | |
| c9: | IF A.162/53 AND A.163/17 THEN m ELSE n/a - - the SIP Referred-By mechanism and REFER response. | | | | | | |
| c10: | IF A.3/2 THEN m ELSE i - - P-CSCF. | | | | | | |
| c19: | IF A.162/51 THEN i ELSE n/a - - an event state publication extension to the session initiation protocol. | | | | | | |
| c20: | IF A.162/51 THEN m ELSE n/a - - an event state publication extension to the session initiation protocol. | | | | | | |
| p21: | A.164/2 OR A.164/3 OR A.164/4 OR A.164/5 - - 1xx response | | | | | | |
| p22: | A.164/6 OR A.164/7 - - 2xx response | | | | | | |
| p23: | A.164/8 OR A.164/9 OR A.164/10 OR A.164/11 OR A.164/12 OR A.164/13 - - 3xx response | | | | | | |
| p24: | A.164/14 OR A.164/15 OR A.164/16 OR A.164/17 OR A.164/18 OR A.164/19 OR A.164/20 OR A.164/21 OR A.164/22 OR A.164/22A OR A.164/23 OR A.164/24 OR A.164/25 OR A.164/26 OR A.164/27 OR A.164/28 OR A.164/28A OR A.164/29 OR A.164/29A OR A.164/30 OR A.164/31 OR A.164/32 OR A.164/33 OR A.164/34 OR A.164/35 OR A.164/36 OR A.164/436 OR A.164/38 OR A.164/39 OR A.164/40 OR A.164/41 OR A.164/41A. - - 4xx response | | | | | | |
| p25: | A.164/42 OR A.164/43 OR A.164/44 OR A.164/45 OR A.164/46 OR A.164/47 OR A.164/48 OR A.164/49 - - 5xx response | | | | | | |
| p26: | A.164/50 OR A.164/51 OR A.164/52 OR A.164/53 - - 6xx response | | | | | | |

### A.2.2.4.2 ACK method

Prerequisite A.163/1 - - ACK request

**Table A.165: Supported headers within the ACK request**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Accept-Contact | [56B] 9.2 | c10 | c10 | [56B] 9.2 | c11 | c11 |
| 2 | Allow-Events | [28] 7.2.2 | m | m | [28] 7.2.2 | c1 | c1 |
| 3 | Authorization | [26] 20.7 | m | m | [26] 20.7 | i | i |
| 4 | Call-ID | [26] 20.8 | m | m | [26] 20.8 | m | m |
| 6 | Content-Disposition | [26] 20.11 | m | m | [26] 20.11 | i | i |
| 7 | Content-Encoding | [26] 20.12 | m | m | [26] 20.12 | i | i |
| 8 | Content-Language | [26] 20.13 | m | m | [26] 20.13 | i | i |
| 9 | Content-Length | [26] 20.14 | m | m | [26] 20.14 | m | m |
| 10 | Content-Type | [26] 20.15 | m | m | [26] 20.15 | i | c3 |
| 11 | Cseq | [26] 20.16 | m | m | [26] 20.16 | m | m |
| 12 | Date | [26] 20.17 | m | m | [26] 20.17 | c2 | c2 |
| 13 | From | [26] 20.20 | m | m | [26] 20.20 | m | m |
| 14 | Max-Forwards | [26] 20.22 | m | m | [26] 20.22 | m | m |
| 15 | MIME-Version | [26] 20.24 | m | m | [26] 20.24 | i | c3 |
| 15A | Privacy | [33] 4.2 | c6 | c6 | [33] 4.2 | c7 | c7 |
| 16 | Proxy-Authorization | [26] 20.28 | m | m | [26] 20.28 | c4 | c4 |
| 17 | Proxy-Require | [26] 20.29 | m | m | [26] 20.29 | m | m |
| 17A | Reason | [34A] 2 | c8 | c8 | [34A] 2 | c9 | c9 |
| 17B | Reject-Contact | [56B] 9.2 | c10 | c10 | [56B] 9.2 | c11 | c11 |
| 17C | Request-Disposition | [56B] 9.1 | c10 | c10 | [56B] 9.1 | c11 | c11 |
| 18 | Require | [26] 20.32 | m | m | [26] 20.32 | c5 | c5 |
| 19 | Route | [26] 20.34 | m | m | [26] 20.34 | m | m |
| 20 | Timestamp | [26] 20.38 | m | m | [26] 20.38 | i | i |
| 21 | To | [26] 20.39 | m | m | [26] 20.39 | m | m |
| 22 | User-Agent | [26] 20.41 | m | m | [26] 20.41 | i | i |
| 23 | Via | [26] 20.42 | m | m | [26] 20.42 | m | m |
| c1: | IF A.4/20 THEN m ELSE i - - SIP specific event notification extension. | | | | | | |
| c2: | IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses. | | | | | | |
| c3: | IF A.3/2 OR A.3/4 THEN m ELSE i - - P-CSCF or S-CSCF. | | | | | | |
| c4: | IF A.162/8A THEN m ELSE i - - authentication between UA and proxy. | | | | | | |
| c5: | IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER. | | | | | | |
| c6: | IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP). | | | | | | |
| c7: | IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently. | | | | | | |
| c8: | IF A.162/48 THEN m ELSE n/a - - the Reason header field for the session initiation protocol. | | | | | | |
| c9: | IF A.162/48 THEN i ELSE n/a - - the Reason header field for the session initiation protocol. | | | | | | |
| c10: | IF A.162/50 THEN m ELSE n/a - - caller preferences for the session initiation protocol. | | | | | | |
| c11: | IF A.162/50 THEN i ELSE n/a - - caller preferences for the session initiation protocol. | | | | | | |
| NOTE: | c1 refers to the UA role major capability as this is the case of a proxy that also acts as a UA specifically for SUBSCRIBE and NOTIFY. | | | | | | |

Editor's note: Is the following table a suitable way of showing the contents of message bodies.

Prerequisite A.163/1 - - ACK request

**Table A.166: Supported message bodies within the ACK request**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | | | | | | | |

### A.2.2.4.3 BYE method

Prerequisite A.163/2 - - BYE request

**Table A.167: Supported headers within the BYE request**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Accept | [26] 20.1 | m | m | [26] 20.1 | i | i |
| 1A | Accept-Contact | [56B] 9.2 | c22 | c22 | [56B] 9.2 | c23 | c23 |
| 2 | Accept-Encoding | [26] 20.2 | m | m | [26] 20.2 | i | i |
| 3 | Accept-Language | [26] 20.3 | m | m | [26] 20.3 | i | i |
| 3A | Allow | [26] 20.5 | m | m | [26] 20.5 | i | i |
| 4 | Allow-Events | [28] 7.2.2 | m | m | [28] 7.2.2 | c1 | c1 |
| 5 | Authorization | [26] 20.7 | m | m | [26] 20.7 | i | i |
| 6 | Call-ID | [26] 20.8 | m | m | [26] 20.8 | m | m |
| 7 | Content-Disposition | [26] 20.11 | m | m | [26] 20.11 | i | c3 |
| 8 | Content-Encoding | [26] 20.12 | m | m | [26] 20.12 | i | c3 |
| 9 | Content-Language | [26] 20.13 | m | m | [26] 20.13 | i | c3 |
| 10 | Content-Length | [26] 20.14 | m | m | [26] 20.14 | m | m |
| 11 | Content-Type | [26] 20.15 | m | m | [26] 20.15 | i | c3 |
| 12 | Cseq | [26] 20.16 | m | m | [26] 20.16 | m | m |
| 13 | Date | [26] 20.17 | m | m | [26] 20.17 | c2 | c2 |
| 14 | From | [26] 20.20 | m | m | [26] 20.20 | m | m |
| 15 | Max-Forwards | [26] 20.22 | m | m | [26] 20.22 | m | m |
| 16 | MIME-Version | [26] 20.24 | m | m | [26] 20.24 | i | c3 |
| 16A | P-Access-Network-Info | [52] 4.4 | c13 | c13 | [52] 4.4 | c14 | c14 |
| 16B | P-Asserted-Identity | [34] 9.1 | c9 | c9 | [34] 9.1 | c10 | c10 |
| 16C | P-Charging-Function-Addresses | [52] 4.5 | c17 | c17 | [52] 4.5 | c18 | c18 |
| 16D | P-Charging-Vector | [52] 4.6 | c15 | n/a | [52] 4.6 | c16 | n/a |
| 16E | P-Preferred-Identity | [34] 9.2 | x | x | [34] 9.2 | c8 | n/a |
| 16F | Privacy | [33] 4.2 | c11 | c11 | [33] 4.2 | c12 | c12 |
| 17 | Proxy-Authorization | [26] 20.28 | m | m | [26] 20.28 | c4 | c4 |
| 18 | Proxy-Require | [26] 20.29 | m | m | [26] 20.29 | m | m |
| 18A | Reason | [34A] 2 | c20 | c20 | [34A] 2 | c21 | c21 |
| 19 | Record-Route | [26] 20.30 | m | m | [26] 20.30 | c7 | c7 |
| 19A | Referred-By | [59] 3 | c24 | c24 | [59] 3 | c25 | c25 |
| 19B | Reject-Contact | [56B] 9.2 | c22 | c22 | [56B] 9.2 | c23 | c23 |
| 19C | Request-Disposition | [56B] 9.1 | c22 | c22 | [56B] 9.1 | c23 | c23 |
| 20 | Require | [26] 20.32 | m | m | [26] 20.32 | c5 | c5 |
| 21 | Route | [26] 20.34 | m | m | [26] 20.34 | m | m |
| 21A | Security-Client | [48] 2.3.1 | x | x | [48] 2.3.1 | c19 | c19 |
| 21B | Security-Verify | [48] 2.3.1 | x | x | [48] 2.3.1 | c19 | c19 |
| 22 | Supported | [26] 20.37 | m | m | [26] 20.37 | c6 | c6 |
| 23 | Timestamp | [26] 20.38 | m | m | [26] 20.38 | i | i |
| 24 | To | [26] 20.39 | m | m | [26] 20.39 | m | m |
| 25 | User-Agent | [26] 20.41 | m | m | [26] 20.41 | i | i |
| 26 | Via | [26] 20.42 | m | m | [26] 20.42 | m | m |

| | |
|---|---|
| c1: | IF A.4/20 THEN m ELSE i - - SIP specific event notification extension. |
| c2: | IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses. |
| c3: | IF A.3/2 OR A.3/4 THEN m ELSE i - - P-CSCF or S-CSCF. |
| c4: | IF A.162/8A THEN m ELSE i - - authentication between UA and proxy. |
| c5: | IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER. |
| c6: | IF A.162/16 THEN m ELSE i - - reading the contents of the Supported header before proxying the response. |
| c7: | IF A.162/14 THEN o ELSE i - - the requirement to be able to insert itself in the subsequent transactions in a dialog. |
| c8: | IF A.162/30A THEN m ELSE n/a - - act as first entity within the trust domain for asserted identity. |
| c9: | IF A.162/30 THEN m ELSE n/a - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks. |
| c10: | IF A.162/30A or A.162/30B THEN m ELSE i - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks or subsequent entity within trust network that can route outside the trust network. |
| c11: | IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP). |
| c12: | IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently. |
| c13: | IF A.162/43 THEN x ELSE IF A.162/41 THEN m ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension. |
| c14: | IF A.162/43 THEN m ELSE IF A.162/41 THEN i ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension. |
| c15: | IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension. |
| c16: | IF A.162/46 THEN m ELSE IF A.162/45 THEN i ELSE n/a - - adding, deleting, reading or modifying the P-Charging-Vector header before proxying the request or response or the P-Charging-Vector header extension. |
| c17: | IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension. |
| c18: | IF A.162/44A THEN m ELSE IF A.162/44 THEN i ELSE n/a - - adding, deleting or reading the P-Charging-Function-Addresses header before proxying the request or response, or the P-Charging-Function-Addresses header extension. |
| c19: | IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. |
| c20: | IF A.162/48 THEN m ELSE n/a - - the Reason header field for the session initiation protocol. |
| c21: | IF A.162/48 THEN i ELSE n/a - - the Reason header field for the session initiation protocol. |
| c22: | IF A.162/50 THEN m ELSE n/a - - caller preferences for the session initiation protocol. |
| c23: | IF A.162/50 THEN i ELSE n/a - - caller preferences for the session initiation protocol. |
| c24: | IF A.162/53 THEN i ELSE n/a - - the SIP Referred-By mechanism. |
| c25: | IF A.162/53 THEN m ELSE n/a - - the SIP Referred-By mechanism. |
| NOTE: | c1 refers to the UA role major capability as this is the case of a proxy that also acts as a UA specifically for SUBSCRIBE and NOTIFY. |

Prerequisite A.163/2 - - BYE request

**Table A.168: Supported message bodies within the BYE request**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | | | | | | | |

**Table A.169: Void**

Prerequisite A.163/3 - - BYE response

**Table A.170: Supported headers within the BYE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 0A | Allow | [26] 20.5 | m | m | [26] 20.5 | i | i |
| 1 | Call-ID | [26] 20.8 | m | m | [26] 20.8 | m | m |
| 2 | Content-Disposition | [26] 20.11 | m | m | [26] 20.11 | i | c2 |
| 3 | Content-Encoding | [26] 20.12 | m | m | [26] 20.12 | i | c2 |
| 4 | Content-Language | [26] 20.13 | m | m | [26] 20.13 | i | c2 |
| 5 | Content-Length | [26] 20.14 | m | m | [26] 20.14 | m | m |
| 6 | Content-Type | [26] 20.15 | m | m | [26] 20.15 | i | c2 |
| 7 | Cseq | [26] 20.16 | m | m | [26] 20.16 | m | m |
| 8 | Date | [26] 20.17 | m | m | [26] 20.17 | c1 | c1 |
| 9 | From | [26] 20.20 | m | m | [26] 20.20 | m | m |
| 10 | MIME-Version | [26] 20.24 | m | m | [26] 20.24 | i | c2 |
| 10A | P-Access-Network-Info | [52] 4.4 | c12 | c12 | [52] 4.4 | c13 | c13 |
| 10B | P-Asserted-Identity | [34] 9.1 | c4 | c4 | [34] 9.1 | c5 | c5 |
| 10C | P-Charging-Function-Addresses | [52] 4.5 | c10 | c10 | [52] 4.5 | c11 | c11 |
| 10D | P-Charging-Vector | [52] 4.6 | c8 | n/a | [52] 4.6 | c9 | n/a |
| 10E | P-Preferred-Identity | [34] 9.2 | x | x | [34] 9.2 | c3 | n/a |
| 10F | Privacy | [33] 4.2 | c6 | c6 | [33] 4.2 | c7 | c7 |
| 10G | Require | [26] 20.32 | m | m | [26] 20.32 | c14 | c14 |
| 10H | Server | [26] 20.35 | m | m | [26] 20.35 | i | i |
| 11 | Timestamp | [26] 20.38 | m | m | [26] 20.38 | i | i |
| 12 | To | [26] 20.39 | m | m | [26] 20.39 | m | m |
| 12A | User-Agent | [26] 20.41 | m | m | [26] 20.41 | i | i |
| 13 | Via | [26] 20.42 | m | m | [26] 20.42 | m | m |
| 14 | Warning | [26] 20.43 | m | m | [26] 20.43 | i | i |

c1: IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses.
c2: IF A.3/2 OR A.3/4 THEN m ELSE i - - P-CSCF or S-CSCF.
c3: IF A.162/30A THEN m ELSE n/a - - act as first entity within the trust domain for asserted identity.
c4: IF A.162/30 THEN m ELSE n/a - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.
c5: IF A.162/30A or A.162/30B THEN m ELSE i - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks or subsequent entity within trust network that can route outside the trust network.
c6: IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c7: IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently.
c8: IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.
c9: IF A.162/46 THEN m ELSE IF A.162/45 THEN i ELSE n/a - - adding, deleting, reading or modifying the P-Charging-Vector header before proxying the request or response or the P-Charging-Vector header extension.
c10: IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.
c11: IF A.162/44A THEN m ELSE IF A.162/44 THEN i ELSE n/a - - adding, deleting or reading the P-Charging-Function-Addresses header before proxying the request or response, or the P-Charging-Function-Addresses header extension.
c12: IF A.162/43 THEN x ELSE IF A.162/41 THEN m ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.
c13: IF A.162/43 THEN m ELSE IF A.162/41 THEN i ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.
c14: IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER.

Prerequisite A.163/3 - - BYE response

Prerequisite: A.164/102 - - Additional for 2xx response

**Table A.171: Supported headers within the BYE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 0A | Allow-Events | [28] 7.2.2 | m | m | [28] 7.2.2 | i | c1 |
| 1 | Authentication-Info | [26] 20.6 | m | m | [26] 20.6 | i | i |
| 2 | Record-Route | [26] 20.30 | m | m | [26] 20.30 | c3 | c3 |
| 5 | Supported | [26] 20.37 | m | m | [26] 20.37 | i | i |
| c1: | IF A.4/20 THEN m ELSE i - - SIP specific event notification extension. | | | | | | |
| c3: | IF A.162/15 THEN o ELSE i - - the requirement to be able to use separate URIs in the upstream direction and downstream direction when record routeing. | | | | | | |

Prerequisite A.163/3 - - BYE response

Prerequisite: A.164/103 OR A.164/104 OR A.164/105 OR A.164/106 - - Additional for 3xx – 6xx response

**Table A.171A: Supported headers within the BYE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Error-Info | [26] 20.18 | m | m | [26] 20.18 | i | i |

Prerequisite A.163/3 - BYE response

Prerequisite: A.164/103 OR A.164/35 - - Additional for 3xx or 485 (Ambiguous) response

**Table A.172: Supported headers within the BYE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Contact | [26] 20.10 | m | m | [26] 20.10 | c1 | c1 |
| c1: | IF A.162/19E THEN m ELSE i - - deleting Contact headers. | | | | | | |

Prerequisite A.163/3 - - BYE response

Prerequisite: A.164/14 - - Additional for 401 (Unauthorized) response

**Table A.173: Supported headers within the BYE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 2 | Proxy-Authenticate | [26] 20.27 | m | m | [26] 20.27 | m | m |
| 8 | WWW-Authenticate | [26] 20.44 | m | m | [26] 20.44 | i | i |

Prerequisite A.163/3 - - BYE response

Prerequisite: A.164/17 OR A.164/23 OR A.164/30 OR A.164/36 OR A.164/42 OR A.164/45 OR A.164/50 OR A.164/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response

**Table A.174: Supported headers within the BYE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 3 | Retry-After | [26] 20.33 | m | m | [26] 20.33 | i | i |

**Table A.175: Void**

Prerequisite A.163/3 - - BYE response

Prerequisite: A.164/20 - - Additional for 407 (Proxy Authentication Required) response

**Table A.176: Supported headers within the BYE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 2 | Proxy-Authenticate | [26] 20.27 | m | m | [26] 20.27 | m | m |
| 6 | WWW-Authenticate | [26] 20.44 | m | m | [26] 20.44 | i | i |

Prerequisite A.163/3 - - BYE response

Prerequisite: A.164/25 - - Additional for 415 (Unsupported Media Type) response

**Table A.177: Supported headers within the BYE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Accept | [26] 20.1 | m | m | [26] 20.1 | i | i |
| 2 | Accept-Encoding | [26] 20.2 | m | m | [26] 20.2 | i | i |
| 3 | Accept-Language | [26] 20.3 | m | m | [26] 20.3 | i | i |

Prerequisite A.163/3 - - BYE response

Prerequisite: A.164/27 - - Additional for 420 (Bad Extension) response

**Table A.178: Supported headers within the BYE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 5 | Unsupported | [26] 20.40 | m | m | [26] 20.40 | c3 | c3 |
| c3: | IF A.162/18 THEN m ELSE i - - reading the contents of the Unsupported header before proxying the 420 response to a method other than REGISTER. | | | | | | |

Prerequisite A.163/3 - - BYE response

Prerequisite: A.164/28 OR A.164/41A - - Additional for 421 (Extension Required), 494 (Security Agreement Required) response

**Table A.178A: Supported headers within the BYE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 3 | Security-Server | [48] 2 | c1 | c1 | [48] 2 | n/a | n/a |
| c1: | IF A.162/47 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. | | | | | | |

**Table A.179: Void**

Prerequisite A.163/3 - - BYE response

**Table A.180: Supported message bodies within the BYE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | | | | | | | |

### A.2.2.4.4 CANCEL method

Prerequisite A.163/4 - - CANCEL request

**Table A.181: Supported headers within the CANCEL request**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Accept-Contact | [56B] 9.2 | c10 | c10 | [56B] 9.2 | c11 | c11 |
| 5 | Authorization | [26] 20.7 | m | m | [26] 20.7 | i | i |
| 6 | Call-ID | [26] 20.8 | m | m | [26] 20.8 | m | m |
| 8 | Content-Length | [26] 20.14 | m | m | [26] 20.14 | m | m |
| 9 | Cseq | [26] 20.16 | m | m | [26] 20.16 | m | m |
| 10 | Date | [26] 20.17 | m | m | [26] 20.17 | c2 | c2 |
| 11 | From | [26] 20.20 | m | m | [26] 20.20 | m | m |
| 12 | Max-Forwards | [26] 20.22 | m | m | [26] 20.22 | m | m |
| 14 | Privacy | [33] 4.2 | c3 | c3 | [33] 4.2 | c4 | c4 |
| 15 | Reason | [34A] 2 | c8 | c8 | [34A] 2 | c9 | c9 |
| 16 | Record-Route | [26] 20.30 | m | m | [26] 20.30 | c7 | c7 |
| 17 | Reject-Contact | [56B] 9.2 | c10 | c10 | [56B] 9.2 | c11 | c11 |
| 17A | Request-Disposition | [56B] 9.1 | c10 | c10 | [56B] 9.1 | c11 | c11 |
| 18 | Route | [26] 20.34 | m | m | [26] 20.34 | m | m |
| 19 | Supported | [26] 20.37 | m | m | [26] 20.37 | c6 | c6 |
| 20 | Timestamp | [26] 20.38 | m | m | [26] 20.38 | i | i |
| 21 | To | [26] 20.39 | m | m | [26] 20.39 | m | m |
| 22 | User-Agent | [26] 20.41 | m | m | [26] 20.41 | i | i |
| 23 | Via | [26] 20.42 | m | m | [26] 20.42 | m | m |
| c2: | IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses. | | | | | | |
| c3: | IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP). | | | | | | |
| c4: | IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently. | | | | | | |
| c6: | IF A.162/16 THEN m ELSE i - - reading the contents of the Supported header before proxying the response. | | | | | | |
| c7: | IF A.162/14 THEN o ELSE i - - the requirement to be able to insert itself in the subsequent transactions in a dialog. | | | | | | |
| c8: | IF A.162/48 THEN m ELSE n/a - - the Reason header field for the session initiation protocol. | | | | | | |
| c9: | IF A.162/48 THEN i ELSE n/a - - the Reason header field for the session initiation protocol. | | | | | | |
| c10: | IF A.162/50 THEN m ELSE n/a - - caller preferences for the session initiation protocol. | | | | | | |
| c11: | IF A.162/50 THEN i ELSE n/a - - caller preferences for the session initiation protocol. | | | | | | |
| NOTE: | c1 refers to the UA role major capability as this is the case of a proxy that also acts as a UA specifically for SUBSCRIBE and NOTIFY. | | | | | | |

Prerequisite A.163/4 - - CANCEL request

**Table A.182: Supported message bodies within the CANCEL request**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | | | | | | | |

Prerequisite A.163/5 - - CANCEL response for all status-codes

**Table A.183: Supported headers within the CANCEL response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Call-ID | [26] 20.8 | m | m | [26] 20.8 | m | m |
| 2 | Content-Length | [26] 20.14 | m | m | [26] 20.14 | m | m |
| 3 | Cseq | [26] 20.16 | m | m | [26] 20.16 | m | m |
| 4 | Date | [26] 20.17 | m | m | [26] 20.17 | c1 | c1 |
| 5 | From | [26] 20.20 | m | m | [26] 20.20 | m | m |
| 5A | Privacy | [33] 4.2 | c2 | c2 | [33] 4.2 | c3 | c3 |
| 6 | Timestamp | [26] 20.38 | m | m | [26] 20.38 | i | i |
| 7 | To | [26] 20.39 | m | m | [26] 20.39 | m | m |
| 7A | User-Agent | [26] 20.41 | o | | [26] 20.41 | o | |
| 8 | Via | [26] 20.42 | m | m | [26] 20.42 | m | m |
| 9 | Warning | [26] 20.43 | m | m | [26] 20.43 | i | i |
| c1: | IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses. | | | | | | |
| c2: | IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP). | | | | | | |
| c3: | IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently. | | | | | | |

Prerequisite A.163/5 - - CANCEL response

Prerequisite: A.164/102 - - Additional for 2xx response

**Table A.184: Supported headers within the CANCEL response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 2 | Record-Route | [26] 20.30 | m | m | [26] 20.30 | c3 | c3 |
| 4 | Supported | [26] 20.37 | m | m | [26] 20.37 | i | i |
| c3: | IF A.162/15 THEN o ELSE i - - the requirement to be able to use separate URIs in the upstream direction and downstream direction when record routeing. | | | | | | |

Prerequisite A.163/5 - - CANCEL response

Prerequisite: A.164/103 OR A.164/104 OR A.164/105 OR A.164/106 - - Additional for 3xx – 6xx response

**Table A.184A: Supported headers within the CANCEL response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Error-Info | [26] 20.18 | m | m | [26] 20.18 | i | i |

**Table A.185: Void**

Prerequisite A.163/5 - - CANCEL response

Prerequisite: A.164/17 OR A.164/23 OR A.164/30 OR A.164/42 OR A.164/45 OR A.164/50 OR A.164/51 - - Additional for Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response

**Table A.186: Supported headers within the CANCEL response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 4 | Retry-After | [26] 20.33 | m | m | [26] 20.33 | i | i |

**Table A.188: Void**

Prerequisite A.163/5 - - CANCEL response

**Table A.189: Supported message bodies within the CANCEL response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | | | | | | | |

### A.2.2.4.5 COMET method

Void

### A.2.2.4.6 INFO method

Void

### A.2.2.4.7 INVITE method

Prerequisite A.163/8 - - INVITE request

**Table A.204: Supported headers within the INVITE request**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Accept | [26] 20.1 | m | m | [26] 20.1 | i | i |
| 1A | Accept-Contact | [56B] 9.2 | c34 | c34 | [56B] 9.2 | c34 | c35 |
| 2 | Accept-Encoding | [26] 20.2 | m | m | [26] 20.2 | i | i |
| 3 | Accept-Language | [26] 20.3 | m | m | [26] 20.3 | i | i |
| 4 | Alert-Info | [26] 20.4 | c2 | c2 | [26] 20.4 | c3 | c3 |
| 5 | Allow | [26] 20.5 | m | m | [26] 20.5 | i | i |
| 6 | Allow-Events | [28] 7.2.2 | m | m | [28] 7.2.2 | c1 | c1 |
| 8 | Authorization | [26] 20.7 | m | m | [26] 20.7 | i | i |
| 9 | Call-ID | [26] 20.8 | m | m | [26] 20.8 | m | m |
| 10 | Call-Info | [26] 20.9 | m | m | [26] 20.9 | c12 | c12 |
| 11 | Contact | [26] 20.10 | m | m | [26] 20.10 | i | i |
| 12 | Content-Disposition | [26] 20.11 | m | m | [26] 20.11 | i | c6 |
| 13 | Content-Encoding | [26] 20.12 | m | m | [26] 20.12 | i | c6 |
| 14 | Content-Language | [26] 20.13 | m | m | [26] 20.13 | i | c6 |
| 15 | Content-Length | [26] 20.14 | m | m | [26] 20.14 | m | m |
| 16 | Content-Type | [26] 20.15 | m | m | [26] 20.15 | i | c6 |
| 17 | Cseq | [26] 20.16 | m | m | [26] 20.16 | m | m |
| 18 | Date | [26] 20.17 | m | m | [26] 20.17 | c4 | c4 |
| 19 | Expires | [26] 20.19 | m | m | [26] 20.19 | i | i |
| 20 | From | [26] 20.20 | m | m | [26] 20.20 | m | m |
| 21 | In-Reply-To | [26] 20.21 | m | m | [26] 20.21 | i | i |
| 21A | Replaces | [61] 7.1 | c41 | c41 | [61] 7.1 | c42 | c42 |
| 22 | Max-Forwards | [26] 20.22 | m | m | [26] 20.22 | m | m |
| 23 | MIME-Version | [26] 20.24 | m | m | [26] 20.24 | i | c6 |
| 23A | Min-SE | [58] 5 | o | o | [58] 5 | o | o |
| 24 | Organization | [26] 20.25 | m | m | [26] 20.25 | c5 | c5 |
| 24A | P-Access-Network-Info | [52] 4.4 | c28 | c28 | [52] 4.4 | c29 | c30 |
| 24B | P-Asserted-Identity | [34] 9.1 | c15 | c15 | [34] 9.1 | c16 | c16 |
| 24C | P-Called-Party-ID | [52] 4.2 | c19 | c19 | [52] 4.2 | c20 | c21 |
| 24D | P-Charging-Function-Addresses | [52] 4.5 | c26 | c27 | [52] 4.5 | c26 | c27 |
| 24E | P-Charging-Vector | [52] 4.6 | c24 | c24 | [52] 4.6 | c25 | c25 |
| 25 | P-Media-Authorization | [31] 5.1 | c9 | c10 | [31] 5.1 | n/a | n/a |
| 25A | P-Preferred-Identity | [34] 9.2 | x | x | [34] 9.2 | c14 | c14 |
| 25B | P-Visited-Network-ID | [52] 4.3 | c22 | n/a | [52] 4.3 | c23 | n/a |
| 26 | Priority | [26] 20.26 | m | m | [26] 20.26 | i | i |
| 26A | Privacy | [33] 4.2 | c17 | c17 | [33] 4.2 | c18 | c18 |
| 27 | Proxy-Authorization | [26] 20.28 | m | m | [26] 20.28 | c13 | c13 |
| 28 | Proxy-Require | [26] 20.29, [34] 4 | m | m | [26] 20.29, [34] 4 | m | m |
| 28A | Reason | [34A] 2 | c32 | c32 | [34A] 2 | c33 | c33 |
| 29 | Record-Route | [26] 20.30 | m | m | [26] 20.30 | c11 | c11 |
| 30 | Referred-By | [59] 3 | c37 | c37 | [59] 3 | c38 | c38 |
| 31 | Reject-Contact | [56B] 9.2 | c34 | c34 | [56B] 9.2 | c34 | c35 |
| 31A | Replaces | [60] 6.1 | c39 | c39 | [60] 6.1 | c40 | c40 |
| 31B | Reply-To | [26] 20.31 | m | m | [26] 20.31 | i | i |

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 31B | Request-Disposition | [56B] 9.1 | c34 | c34 | [56B] 9.1 | c34 | c34 |
| 32 | Require | [26] 20.32 | m | m | [26] 20.32 | c7 | c7 |
| 33 | Route | [26] 20.34 | m | m | [26] 20.34 | m | m |
| 33A | Security-Client | [48] 2.3.1 | x | x | [48] 2.3.1 | c31 | c31 |
| 33B | Security-Verify | [48] 2.3.1 | x | x | [48] 2.3.1 | c31 | c31 |
| 33C | Session-Expires | [58] 4 | c36 | c36 | [58] 4 | c36 | c36 |
| 34 | Subject | [26] 20.36 | m | m | [26] 20.36 | i | i |
| 35 | Supported | [26] 20.37 | m | m | [26] 20.37 | c8 | c8 |
| 36 | Timestamp | [26] 20.38 | m | m | [26] 20.38 | i | i |
| 37 | To | [26] 20.39 | m | m | [26] 20.39 | m | m |
| 38 | User-Agent | [26] 20.41 | m | m | [26] 20.41 | i | i |
| 39 | Via | [26] 20.42 | m | m | [26] 20.42 | m | m |

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| c1: | IF A.4/20 THEN m ELSE i - - SIP specific event notification extension. | | | | | | |
| c2: | IF A.162/10 THEN n/a ELSE m - - suppression or modification of alerting information data. | | | | | | |
| c3: | IF A.162/10 THEN m ELSE i - - suppression or modification of alerting information data. | | | | | | |
| c4: | IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses. | | | | | | |
| c5: | IF A.162/19A OR A.162/19B THEN m ELSE i - - reading, adding or concatenating the Organization header. | | | | | | |
| c6: | IF A.3/2 OR A.3/4 THEN m ELSE i - - P-CSCF or S-CSCF. | | | | | | |
| c7: | IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER. | | | | | | |
| c8: | IF A.162/16 THEN m ELSE i - - reading the contents of the Supported header before proxying the response. | | | | | | |
| c9: | IF A.162/26 THEN m ELSE n/a - - SIP extensions for media authorization. | | | | | | |
| c10: | IF A.3/2 THEN m ELSE n/a - - P-CSCF. | | | | | | |
| c11: | IF A.162/14 THEN m ELSE i - - the requirement to be able to insert itself in the subsequent transactions in a dialog. | | | | | | |
| c12: | IF A.162/19C OR A.162/19D THEN m ELSE i - - reading, adding or concatenating the Call-Info header. | | | | | | |
| c13: | IF A.162/8A THEN m ELSE i - - authentication between UA and proxy. | | | | | | |
| c14: | IF A.162/30A THEN m ELSE n/a - - act as first entity within the trust domain for asserted identity. | | | | | | |
| c15: | IF A.162/30 THEN m ELSE n/a - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks. | | | | | | |
| c16: | IF A.162/30A or A.162/30B THEN m ELSE i - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks or subsequent entity within trust network that can route outside the trust network. | | | | | | |
| c17: | IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP). | | | | | | |
| c18: | IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently. | | | | | | |
| c19: | IF A.162/37 THEN m ELSE n/a - - the P-Called-Party-ID header extension. | | | | | | |
| c20: | IF A.162/37 THEN i ELSE n/a - - the P-Called-Party-ID header extension. | | | | | | |
| c21: | IF A.162/37 AND A.3/2 THEN m ELSE IF A.162/37 AND A.3/3 THEN i ELSE n/a - - the P-Called-Party-ID header extension and P-CSCF or I-CSCF. | | | | | | |
| c22: | IF A.162/38 THEN m ELSE n/a - - the P-Visited-Network-ID header extension. | | | | | | |
| c23: | IF A.162/39 THEN m ELSE i - - reading, or deleting the P-Visited-Network-ID header before proxying the request or response. | | | | | | |
| c24: | IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension. | | | | | | |
| c25: | IF A.162/46 THEN m ELSE IF A.162/45 THEN i ELSE n/a - - adding, deleting, reading or modifying the P-Charging-Vector header before proxying the request or response or the P-Charging-Vector header extension. | | | | | | |
| c26: | IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension. | | | | | | |
| c27: | IF A.162/44A THEN m ELSE IF A.162/44 THEN i ELSE n/a - - adding, deleting or reading the P-Charging-Function-Addresses header before proxying the request or response, or the P-Charging-Function-Addresses header extension. | | | | | | |
| c28: | IF A.162/43 THEN x ELSE IF A.162/41 THEN m ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension. | | | | | | |
| c29: | IF A.162/43 THEN m ELSE IF A.162/41 THEN i ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension. | | | | | | |
| c30: | IF A.162/43 OR (A.162/41 AND A.3/2) THEN m ELSE IF A.162/41 THEN i ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension (with or without P-CSCF). | | | | | | |
| c31: | IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. | | | | | | |
| c32: | IF A.162/48 THEN m ELSE n/a - - the Reason header field for the session initiation protocol. | | | | | | |
| c33: | IF A.162/48 THEN i ELSE n/a - - the Reason header field for the session initiation protocol. | | | | | | |
| c34: | IF A.162/50 THEN m ELSE n/a - - caller preferences for the session initiation protocol. | | | | | | |
| c35: | IF A.162/50 AND A.4/3 THEN m ELSE IF A.162/50 AND NOT A.4/3 THEN i ELSE n/a - - caller preferences for the session initiation protocol, and S-CSCF. | | | | | | |
| c36: | IF A.162/52 THEN m ELSE n/a - - the SIP session timer. | | | | | | |
| c37: | IF A.162/53 THEN i ELSE n/a - - the SIP Referred-By mechanism. | | | | | | |
| c38: | IF A.162/53 THEN m ELSE n/a - - the SIP Referred-By mechanism. | | | | | | |
| c39: | IF A.162/54 THEN m ELSE n/a - - the Session Inititation Protocol (SIP) "Replaces" header. | | | | | | |
| c40: | IF A.162/54 THEN i ELSE n/a - - the Session Inititation Protocol (SIP) "Replaces" header. | | | | | | |
| c41: | IF A.162/55 THEN m ELSE n/a - - the Session Inititation Protocol (SIP) "Join" header. | | | | | | |
| c42: | IF A.162/55 THEN i ELSE n/a - - the Session Inititation Protocol (SIP) "Join" header. | | | | | | |
| NOTE: | c1 refers to the UA role major capability as this is the case of a proxy that also acts as a UA specifically for SUBSCRIBE and NOTIFY. | | | | | | |

Prerequisite A.163/8 - - INVITE request

**Table A.205: Supported message bodies within the INVITE request**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | | | | | | | |

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/1 - - Additional for 100 (Trying) response

**Table A.206: Supported headers within the INVITE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Call-ID | [26] 20.8 | m | m | [26] 20.8 | m | m |
| 2 | Content-Length | [26] 20.14 | m | m | [26] 20.14 | m | m |
| 3 | Cseq | [26] 20.16 | m | m | [26] 20.16 | m | m |
| 4 | Date | [26] 20.17 | c1 | c1 | [26] 20.17 | c2 | c2 |
| 5 | From | [26] 20.20 | m | m | [26] 20.20 | m | m |
| 6 | To | [26] 20.39 | m | m | [26] 20.39 | m | m |
| 7 | Via | [26] 20.42 | m | m | [26] 20.42 | m | m |
| c1: | IF (A.162/9 AND A.162/5) OR A.162/4 THEN m ELSE n/a - - stateful proxy behaviour that inserts date, or stateless proxies. | | | | | | |
| c2: | IF A.162/4 THEN i ELSE m - - Stateless proxy passes on. | | | | | | |

Prerequisite A.163/9 - - INVITE response for all remaining status-codes

**Table A.207: Supported headers within the INVITE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 0A | Allow | [26] 20.5 | m | m | [26] 20.5 | i | i |
| 1 | Call-ID | [26] 20.8 | m | m | [26] 20.8 | m | m |
| 1A | Call-Info | [26] 20.9 | m | m | [26] 20.9 | c4 | c4 |
| 2 | Content-Disposition | [26] 20.11 | m | m | [26] 20.11 | i | c3 |
| 3 | Content-Encoding | [26] 20.12 | m | m | [26] 20.12 | i | c3 |
| 4 | Content-Language | [26] 20.13 | m | m | [26] 20.13 | i | c3 |
| 5 | Content-Length | [26] 20.14 | m | m | [26] 20.14 | m | m |
| 6 | Content-Type | [26] 20.15 | m | m | [26] 20.15 | i | c3 |
| 7 | Cseq | [26] 20.16 | m | m | [26] 20.16 | m | m |
| 8 | Date | [26] 20.17 | m | m | [26] 20.17 | c1 | c1 |
| 8A | Expires | [26] 20.19 | m | m | [26] 20.19 | i | i |
| 9 | From | [26] 20.20 | m | m | [26] 20.20 | m | m |
| 10 | MIME-Version | [26] 20.24 | m | m | [26] 20.24 | i | c3 |
| 11 | Organization | [26] 20.25 | m | m | [26] 20.25 | c2 | c2 |
| 11A | P-Access-Network-Info | [52] 4.4 | c14 | c14 | [52] 4.4 | c15 | c15 |
| 11B | P-Asserted-Identity | [34] 9.1 | c6 | c6 | [34] 9.1 | c7 | c7 |
| 11C | P-Charging-Function-Addresses | [52] 4.5 | c12 | c12 | [52] 4.5 | c13 | c13 |
| 11D | P-Charging-Vector | [52] 4.6 | c10 | c10 | [52] 4.6 | c11 | c11 |
| 11E | P-Preferred-Identity | [34] 9.2 | x | x | [34] 9.2 | c5 | n/a |
| 11F | Privacy | [33] 4.2 | c8 | c8 | [33] 4.2 | c9 | c9 |
| 11G | Reply-To | [26] 20.31 | m | m | [26] 20.31 | i | i |
| 11H | Require | [26] 20.32 | m | m | [26] 20.32 | c16 | c16 |
| 11I | Server | [26] 20.35 | m | m | [26] 20.35 | i | i |
| 12 | Timestamp | [26] 20.38 | m | m | [26] 20.38 | i | i |
| 13 | To | [26] 20.39 | m | m | [26] 20.39 | m | m |
| 13A | User-Agent | [26] 20.41 | m | m | [26] 20.41 | i | i |
| 14 | Via | [26] 20.42 | m | m | [26] 20.42 | m | m |
| 15 | Warning | [26] 20.43 | m | m | [26] 20.43 | i | i |

c1: IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses.
c2: IF A.162/19A OR A.162/19B THEN m ELSE i - - reading, adding or concatenating the Organization header.
c3: IF A.3/2 OR A.3/4 THEN m ELSE i - - P-CSCF or S-CSCF.
c4: IF A.162/19C OR A.162/19D THEN m ELSE i - - reading, adding or concatenating the Call-Info header.
c5: IF A.162/30A THEN m ELSE n/a - - act as first entity within the trust domain for asserted identity.
c6: IF A.162/30 THEN m ELSE n/a - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.
c7: IF A.162/30A or A.162/30B THEN m ELSE i - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks or subsequent entity within trust network that can route outside the trust network.
c8: IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c9: IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently.
c10: IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.
c11: IF A.162/46 THEN m ELSE IF A.162/45 THEN i ELSE n/a - - adding, deleting, reading or modifying the P-Charging-Vector header before proxying the request or response or the P-Charging-Vector header extension.
c12: IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.
c13: IF A.162/44A THEN m ELSE IF A.162/44 THEN i ELSE n/a - - adding, deleting or reading the P-Charging-Function-Addresses header before proxying the request or response, or the P-Charging-Function-Addresses header extension.
c14: IF A.162/43 THEN x ELSE IF A.162/41 THEN m ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.
c15: IF A.162/43 THEN m ELSE IF A.162/41 THEN i ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.
c16: IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER.

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/101 - - Additional for 1xx response

**Table A.208: Supported headers within the INVITE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 4 | Contact | [26] 20.10 | m | m | [26] 20.10 | i | i |
| 6 | P-Media-Authorization | [31] 5.1 | c9 | c10 | [31] 5.1 | n/a | n/a |
| 9 | Rseq | [27] 7.1 | m | m | [27] 7.1 | i | i |
| 11 | Supported | [26] 20.37 | m | m | [26] 20.37 | i | i |
| c9: | IF A.162/26 THEN m ELSE n/a - - SIP extensions for media authorization. | | | | | | |
| c10: | IF A.3/2 THEN m ELSE n/a - - P-CSCF. | | | | | | |

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/102 - - Additional for 2xx response

**Table A.209: Supported headers within the INVITE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Accept | [26] 20.1 | m | m | [26] 20.1 | i | i |
| 1A | Accept-Encoding | [26] 20.2 | m | m | [26] 20.2 | i | i |
| 1B | Accept-Language | [26] 20.3 | m | m | [26] 20.3 | i | i |
| 2 | Allow-Events | [28] 7.2.2 | m | m | [28] 7.2.2 | c1 | c1 |
| 4 | Authentication-Info | [26] 20.6 | m | m | [26] 20.6 | i | i |
| 6 | Contact | [26] 20.10 | m | m | [26] 20.10 | i | i |
| 8 | P-Media-Authorization | [31] 5.1 | c9 | c10 | [31] 5.1 | n/a | n/a |
| 9 | Record-Route | [26] 20.30 | m | m | [26] 20.30 | c3 | c3 |
| 10 | Session-Expires | [58] 4 | c11 | c11 | [58] 4 | c11 | c11 |
| 13 | Supported | [26] 20.37 | m | m | [26] 20.37 | i | i |
| c1: | IF A.4/20 THEN m ELSE i - - SIP specific event notification extension. | | | | | | |
| c3: | IF A.162/14 THEN m ELSE i - - the requirement to be able to insert itself in the subsequent transactions in a dialog. | | | | | | |
| c9: | IF A.162/26 THEN m ELSE n/a - - SIP extensions for media authorization. | | | | | | |
| c10: | IF A.3/2 THEN m ELSE n/a - - P-CSCF. | | | | | | |
| c11: | IF A.162/52 THEN m ELSE n/a - - the SIP session timer. | | | | | | |

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/103 OR A.164/104 OR A.164/105 OR A.164/106 - - Additional for 3xx – 6xx response

**Table A.209A: Supported headers within the INVITE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Error-Info | [26] 20.18 | m | m | [26] 20.18 | i | i |

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/103 OR A.164/35 - - Additional for 3xx or 485 (Ambiguous) response

**Table A.210: Supported headers within the INVITE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 4 | Contact | [26] 20.10 | m | m | [26] 20.10 | c1 | c1 |
| c1: | IF A.162/19E THEN m ELSE i - - deleting Contact headers. | | | | | | |

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/14 - - Additional for 401 (Unauthorized) response

**Table A.211: Supported headers within the INVITE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 6 | Proxy-Authenticate | [26] 20.27 | m | m | [26] 20.27 | m | m |
| 15 | WWW-Authenticate | [26] 20.44 | o | | [26] 20.44 | o | |

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/17 OR A.164/23 OR A.164/30 OR A.164/36 OR A.164/50 OR A.164/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 600 (Busy Everywhere), 603 (Decline) response

**Table A.212: Supported headers within the INVITE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 8 | Retry-After | [26] 20.33 | m | m | [26] 20.33 | i | i |
| 12 | Via | [26] 20.42 | m | m | [26] 20.42 | m | m |

**Table A.213: Void**

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/20 - - Additional for 407 (Proxy Authentication Required) response

**Table A.214: Supported headers within the INVITE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 6 | Proxy-Authenticate | [26] 20.27 | m | m | [26] 20.27 | m | m |
| 11 | WWW-Authenticate | [26] 20.44 | m | m | [26] 20.44 | i | i |

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/25 - - Additional for 415 (Unsupported Media Type) response

**Table A.215: Supported headers within the INVITE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Accept | [26] 20.1 | m | m | [26] 20.1 | i | i |
| 2 | Accept-Encoding | [26] 20.2 | m | m | [26] 20.2 | i | i |
| 3 | Accept-Language | [26] 20.3 | m | m | [26] 20.3 | i | i |

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/27 - - Additional for 420 (Bad Extension) response

**Table A.216: Supported headers within the INVITE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 10 | Unsupported | [26] 20.40 | m | m | [26] 20.40 | c3 | c3 |
| c3: | IF A.162/18 THEN m ELSE i - - reading the contents of the Unsupported header before proxying the 420 response to a method other than REGISTER. | | | | | | |

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/28 OR A.164/41A - - Additional for 421 (Extension Required), 494 (Security Agreement Required) response

**Table A.216A: Supported headers within the INVITE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 3 | Security-Server | [48] 2 | c1 | c1 | [48] 2 | n/a | n/a |
| c1: | IF A.162/47 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. | | | | | | |

Prerequisite A.16/9 - - INVITE response

Prerequisite: A.164/28A - - Additional for 422 (Session Interval Too Small) response

**Table A.216B: Supported headers within the INVITE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Min-SE | [58] 5 | c1 | c1 | [58] 5 | c1 | c1 |
| c1: | IF A.162/52 THEN m ELSE n/a - - the SIP session timer. | | | | | | |

**Table A.217: Void**

**Table A.217A: Void**

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/45 - - 503 (Service Unavailable)

**Table A.217B: Supported headers within the INVITE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 8 | Retry-After | [26] 20.33 | m | m | [26] 20.33 | i | i |

Prerequisite A.163/9 - - INVITE response

**Table A.218: Supported message bodies within the INVITE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | | | | | | | |

### A.2.2.4.7A MESSAGE method

Prerequisite A.163/9A - - MESSAGE request

**Table A.218A: Supported headers within the MESSAGE request**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Accept-Contact | [56B] 9.2 | c28 | c28 | [56B] 9.2 | c28 | c29 |
| 1A | Allow | [26] 20.5 | m | m | [50] 10 | i | i |
| 2 | Allow-Events | [28] 7.2.2 | m | m | [28] 7.2.2 | c1 | c1 |
| 3 | Authorization | [26] 20.7 | m | m | [26] 20.7 | i | i |
| 4 | Call-ID | [26] 20.8 | m | m | [26] 20.8 | m | m |
| 5 | Call-Info | [26] 20.9 | m | m | [26] 20.9 | c4 | c4 |
| 6 | Content-Disposition | [26] 20.11 | m | m | [26] 20.11 | i | i |
| 7 | Content-Encoding | [26] 20.12 | m | m | [26] 20.12 | i | i |
| 8 | Content-Language | [26] 20.13 | m | m | [26] 20.13 | i | i |
| 9 | Content-Length | [26] 20.14 | m | m | [26] 20.14 | m | m |
| 10 | Content-Type | [26] 20.15 | m | m | [26] 20.15 | i | i |
| 11 | Cseq | [26] 20.16 | m | m | [26] 20.16 | m | m |
| 12 | Date | [26] 20.17 | m | m | [26] 20.17 | c2 | c2 |
| 13 | Expires | [26] 20.19 | m | m | [26] 20.19 | I | i |
| 14 | From | [26] 20.20 | m | m | [26] 20.20 | m | m |
| 15 | In-Reply-To | [26] 20.21 | m | m | [50] 10 | i | i |
| 16 | Max-Forwards | [26] 20.22 | m | m | [26] 20.22 | m | m |
| 17 | MIME-Version | [26] 20.24 | m | m | [26] 20.24 | i | i |
| 18 | Organization | [26] 20.25 | m | m | [26] 20.25 | c3 | c3 |
| 18A | P-Access-Network-Info | [52] 4.4 | c23 | c23 | [52] 4.4 | c24 | c24 |
| 18B | P-Asserted-Identity | [34] 9.1 | c10 | c10 | [34] 9.1 | c11 | c11 |
| 18C | P-Called-Party-ID | [52] 4.2 | c14 | c14 | [52] 4.2 | c15 | c16 |
| 18D | P-Charging-Function-Addresses | [52] 4.5 | c21 | c21 | [52] 4.5 | c22 | c22 |
| 18E | P-Charging-Vector | [52] 4.6 | c19 | c19 | [52] 4.6 | c20 | c20 |
| 18F | P-Preferred-Identity | [34] 9.2 | x | x | [34] 9.2 | c9 | c9 |
| 18G | P-Visited-Network-ID | [52] 4.3 | c17 | n/a | [52] 4.3 | c18 | n/a |
| 19 | Priority | [26] 20.26 | m | m | [26] 20.26 | i | i |
| 19A | Privacy | [33] 4.2 | c12 | c12 | [33] 4.2 | c13 | c13 |
| 20 | Proxy-Authorization | [26] 20.28 | m | m | [26] 20.28 | c8 | c8 |
| 21 | Proxy-Require | [26] 20.29 | m | m | [26] 20.29 | m | m |
| 21A | Reason | [34A] 2 | c26 | c26 | [34A] 2 | c27 | c27 |
| 22 | Record-Route | [26] 20.30 | m | m | [26] 20.30 | c7 | c7 |
| 22A | Referred-By | [59] 3 | c30 | c30 | [59] 3 | c31 | c31 |
| 23 | Reject-Contact | [56B] 9.2 | c28 | c28 | [56B] 9.2 | c28 | c29 |
| 23A | Reply-To | [26] 20.31 | m | m | [26] 20.31 | i | i |
| 23B | Request-Disposition | [56B] 9.1 | c28 | c28 | [56B] 9.1 | c28 | c28 |
| 24 | Require | [26] 20.32 | m | m | [26] 20.32 | c5 | c5 |
| 25 | Route | [26] 20.34 | m | m | [26] 20.34 | m | m |
| 25A | Security-Client | [48] 2.3.1 | x | x | [48] 2.3.1 | c25 | c25 |
| 25B | Security-Verify | [48] 2.3.1 | x | x | [48] 2.3.1 | c25 | c25 |
| 26 | Subject | [26] 20.36 | m | m | [26] 20.36 | i | i |
| 27 | Supported | [26] 20.37 | m | m | [26] 20.37 | c6 | c6 |
| 28 | Timestamp | [26] 20.38 | m | m | [26] 20.38 | i | i |
| 29 | To | [26] 20.39 | m | m | [26] 20.39 | m | m |
| 30 | User-Agent | [26] 20.41 | m | m | [26] 20.41 | i | i |
| 31 | Via | [26] 20.42 | m | m | [26] 20.42 | m | m |

| | |
|---|---|
| c1: | IF A.4/20 THEN m ELSE i - - SIP specific event notification extension. |
| c2: | IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses. |
| c3: | IF A.162/19A OR A.162/19B THEN m ELSE i - - reading, adding or concatenating the Organization header. |
| c4: | IF A.162/19C OR A.162/19D THEN m ELSE i - - reading, adding or concatenating the Call-Info header. |
| c5: | IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER. |
| c6: | IF A.162/16 THEN m ELSE i - - reading the contents of the Supported header before proxying the response. |
| c7: | IF A.162/14 THEN o ELSE i - - the requirement to be able to insert itself in the subsequent transactions in a dialog. |
| c8: | IF A.162/8A THEN m ELSE i - - authentication between UA and proxy. |
| c9: | IF A.162/30A THEN m ELSE n/a - - act as first entity within the trust domain for asserted identity. |
| c10: | IF A.162/30 THEN m ELSE n/a - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks. |
| c11: | IF A.162/30A or A.162/30B THEN m ELSE i - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks or subsequent entity within trust network that can route outside the trust network. |
| c12: | IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP). |
| c13: | IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently. |
| c14: | IF A.162/37 THEN m ELSE n/a - - the P-Called-Party-ID header extension. |
| c15: | IF A.162/37 THEN i ELSE n/a - - the P-Called-Party-ID header extension. |
| c16: | IF A.162/37 AND A.3/2 THEN m ELSE IF A.162/37 AND A.3/3 THEN i ELSE n/a - - the P-Called-Party-ID header extension and P-CSCF or I-CSCF. |
| c17: | IF A.162/38 THEN m ELSE n/a - - the P-Visited-Network-ID header extension. |
| c18: | IF A.162/39 THEN m ELSE i - - reading, or deleting the P-Visited-Network-ID header before proxying the request or response. |
| c19: | IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension. |
| c20: | IF A.162/46 THEN m ELSE IF A.162/45 THEN i ELSE n/a - - adding, deleting, reading or modifying the P-Charging-Vector header before proxying the request or response or the P-Charging-Vector header extension. |
| c21: | IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension. |
| c22: | IF A.162/44A THEN m ELSE IF A.162/44 THEN i ELSE n/a - - adding, deleting or reading the P-Charging-Function-Addresses header before proxying the request or response, or the P-Charging-Function-Addresses header extension. |
| c23: | IF A.162/43 THEN x ELSE IF A.162/41 THEN m ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension. |
| c24: | IF A.162/43 THEN m ELSE IF A.162/41 THEN i ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension. |
| c25: | IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. |
| c26: | IF A.162/48 THEN m ELSE n/a - - the Reason header field for the session initiation protocol. |
| c27: | IF A.162/48 THEN i ELSE n/a - - the Reason header field for the session initiation protocol. |
| c28: | IF A.162/50 THEN m ELSE n/a - - caller preferences for the session initiation protocol. |
| c29: | IF A.162/50 AND A.4/3 THEN m ELSE IF A.162/50 AND NOT A.4/3 THEN i ELSE n/a - - caller preferences for the session initiation protocol, and S-CSCF. |
| c30: | IF A.162/53 THEN i ELSE n/a - - the SIP Referred-By mechanism. |
| c31: | IF A.162/53 THEN m ELSE n/a - - the SIP Referred-By mechanism. |
| NOTE: | c1 refers to the UA role major capability as this is the case of a proxy that also acts as a UA specifically for SUBSCRIBE and NOTIFY. |

Prerequisite A.163/9A - - MESSAGE request

**Table A.218B: Supported message bodies within the MESSAGE request**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | | | | | | | |

Prerequisite A.163/9B - - MESSAGE response for all status-codes

**Table A.218C: Supported headers within the MESSAGE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 0A | Allow | [26] 20.5 | m | m | [26] 20.5 | i | i |
| 1 | Call-ID | [26] 20.8 | m | m | [26] 20.8 | m | m |
| 2 | Call-Info | [26] 20.9 | m | m | [26] 20.9 | c3 | c3 |
| 3 | Content-Disposition | [26] 20.11 | m | m | [26] 20.11 | i | i |
| 4 | Content-Encoding | [26] 20.12 | m | m | [26] 20.12 | i | i |
| 5 | Content-Language | [26] 20.13 | m | m | [26] 20.13 | i | i |
| 6 | Content-Length | [26] 20.14 | m | m | [26] 20.14 | m | m |
| 7 | Content-Type | [26] 20.15 | m | m | [26] 20.15 | i | i |
| 8 | Cseq | [26] 20.16 | m | m | [26] 20.16 | m | m |
| 9 | Date | [26] 20.17 | m | m | [26] 20.17 | c1 | c1 |
| 9A | Expires | [26] 20.19 | m | m | [26] 20.19 | i | i |
| 10 | From | [26] 20.20 | m | m | [26] 20.20 | m | m |
| 11 | MIME-Version | [26] 20.24 | m | m | [26] 20.24 | i | i |
| 12 | Organization | [26] 20.25 | m | m | [26] 20.25 | c2 | c2 |
| 12A | P-Access-Network-Info | [52] 4.4 | c13 | c13 | [52] 4.4 | c14 | c14 |
| 12B | P-Asserted-Identity | [34] 9.1 | c5 | c5 | [34] 9.1 | c6 | c6 |
| 12C | P-Charging-Function-Addresses | [52] 4.5 | c11 | c11 | [52] 4.5 | c12 | c12 |
| 12D | P-Charging-Vector | [52] 4.6 | c9 | n/a | [52] 4.6 | c10 | n/a |
| 12E | P-Preferred-Identity | [34] 9.2 | x | x | [34] 9.2 | c4 | n/a |
| 12F | Privacy | [33] 4.2 | c7 | c7 | [33] 4.2 | c8 | c8 |
| 12G | Reply-To | [26] 20.31 | m | m | [26] 20.31 | i | i |
| 12H | Require | [26] 20.32 | m | m | [26] 20.32 | c15 | c15 |
| 13 | Server | [26] 20.35 | m | m | [26] 20.35 | i | i |
| 14 | Timestamp | [26] 20.38 | i | i | [26] 20.38 | i | i |
| 15 | To | [26] 20.39 | m | m | [26] 20.39 | m | m |
| 16 | User-Agent | [26] 20.41 | m | m | [26] 20.41 | i | i |
| 17 | Via | [26] 20.42 | m | m | [26] 20.42 | m | m |
| 18 | Warning | [26] 20.43 | m | m | [26] 20.43 | i | i |

c1: IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses.
c2: IF A.162/19A OR A.162/19B THEN m ELSE i - - reading, adding or concatenating the Organization header.
c3: IF A.162/19C OR A.162/19D THEN m ELSE i - - reading, adding or concatenating the Call-Info header.
c4: IF A.162/30A THEN m ELSE n/a - - act as first entity within the trust domain for asserted identity.
c5: IF A.162/30 THEN m ELSE n/a - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.
c6: IF A.162/30A or A.162/30B THEN m ELSE i - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks or subsequent entity within trust network that can route outside the trust network.
c7: IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c8: IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently.
c9: IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.
c10: IF A.162/46 THEN m ELSE IF A.162/45 THEN i ELSE n/a - - adding, deleting, reading or modifying the P-Charging-Vector header before proxying the request or response or the P-Charging-Vector header extension.
c11: IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.
c12: IF A.162/44A THEN m ELSE IF A.162/44 THEN i ELSE n/a - - adding, deleting or reading the P-Charging-Function-Addresses header before proxying the request or response, or the P-Charging-Function-Addresses header extension.
c13: IF A.162/43 THEN x ELSE IF A.162/41 THEN m ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.
c14: IF A.162/43 THEN m ELSE IF A.162/41 THEN i ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.
c15: IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER.

Prerequisite A.163/9B - - MESSAGE response

Prerequisite: A.164/102 - - Additional for 2xx response

**Table A.218D: Supported headers within the MESSAGE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Allow-Events | [28] 7.2.2 | m | m | [28] 7.2.2 | c1 | c1 |
| 2 | Authentication-Info | [26] 20.6 | m | m | [26] 20.6 | i | i |
| 4 | Record-Route | [26] 20.30 | m | m | [26] 20.30 | c3 | c3 |
| 6 | Supported | [26] 20.37 | m | m | [26] 20.37 | i | i |
| c1: | IF A.4/20 THEN m ELSE i - - SIP specific event notification extension. | | | | | | |
| c3: | IF A.162/15 THEN o ELSE i - - the requirement to be able to use separate URIs in the upstream direction and downstream direction when record routeing. | | | | | | |

Prerequisite A.163/9B - - MESSAGE response

Prerequisite: A.164/103 OR A.164/104 OR A.164/105 OR A.164/106 - - Additional for 3xx – 6xx response

**Table A.218DA: Supported headers within the MESSAGE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Error-Info | [26] 20.18 | m | m | [26] 20.18 | i | i |

Prerequisite A.163/9B - - MESSAGE response

Prerequisite: A.164/103 OR A.164/35 - - Additional for 3xx or 485 (Ambiguous) response

**Table A.218E: Supported headers within the MESSAGE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 2 | Contact | [26] 20.10 | m | m | [26] 20.10 | c1 | c1 |
| c1: | IF A.162/19E THEN m ELSE i - - deleting Contact headers. | | | | | | |

Prerequisite A.163/9B - - MESSAGE response

Prerequisite: A.164/14 - - Additional for 401 (Unauthorized) response

**Table A.218F: Supported headers within the MESSAGE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 3 | Proxy-Authenticate | [26] 20.27 | m | m | [26] 20.27 | m | m |
| 6 | WWW-Authenticate | [26] 20.44 | m | m | [26] 20.44 | i | i |

Prerequisite A.163/9B - - MESSAGE response

Prerequisite: A.164/17 OR A.164/23 OR A.164/30 OR A.164/36 OR A.164/42 OR A.164/45 OR A.164/50 OR A.164/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response

**Table A.218G: Supported headers within the MESSAGE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 4 | Retry-After | [26] 20.33 | m | m | [26] 20.33 | i | i |

**Table A.218H: Void**

Prerequisite A.163/9B - - MESSAGE response

Prerequisite: A.164/20 - - Additional for 407 (Proxy Authentication Required) response

**Table A.218I: Supported headers within the MESSAGE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 3 | Proxy-Authenticate | [26] 20.27 | m | m | [26] 20.27 | m | m |
| 6 | WWW-Authenticate | [26] 20.44 | m | m | [26] 20.44 | i | i |

Prerequisite A.163/9B - - MESSAGE response

Prerequisite: A.164/25 - - Additional for 415 (Unsupported Media Type)

**Table A.218J: Supported headers within the MESSAGE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Accept | [26] 20.1 | m | m | [26] 20.1 | i | i |
| 2 | Accept-Encoding | [26] 20.2 | m | m | [26] 20.2 | i | i |
| 3 | Accept-Language | [26] 20.3 | m | m | [26] 20.3 | i | i |

Prerequisite A.163/9B - - MESSAGE response

Prerequisite: A.164/27 - - Additional for 420 (Bad Extension) response

**Table A.218K: Supported headers within the MESSAGE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 5 | Unsupported | [26] 20.40 | m | m | [26] 20.40 | c3 | c3 |
| c3: | IF A.162/18 THEN m ELSE i - - reading the contents of the Unsupported header before proxying the 420 response to a method other than REGISTER. | | | | | | |

Prerequisite A.163/9B - - MESSAGE response

Prerequisite: A.164/28 OR A.164/41A - - Additional for 421 (Extension Required), 494 (Security Agreement Required) response

**Table A.218L: Supported headers within the MESSAGE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 3 | Security-Server | [48] 2 | c1 | c1 | [48] 2 | n/a | n/a |
| c1: | IF A.162/47 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. | | | | | | |

**Table A.218M: Void**

Prerequisite A.163/9B - - MESSAGE response

**Table A.218N: Supported message bodies within the MESSAGE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | | | | | | | |

### A.2.2.4.8 NOTIFY method

Prerequisite A.163/10 - - NOTIFY request

**Table A.219: Supported headers within the NOTIFY request**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Accept | [26] 20.1 | m | m | [26] 20.1 | i | i |
| 1A | Accept-Contact | [56B] 9.2 | c21 | c21 | [56B] 9.2 | c22 | c22 |
| 2 | Accept-Encoding | [26] 20.2 | m | m | [26] 20.2 | i | i |
| 3 | Accept-Language | [26] 20.3 | m | m | [26] 20.3 | i | i |
| 3A | Allow | [26] 20.5 | m | m | [26] 20.5 | i | i |
| 4 | Allow-Events | [28] 7.2.2 | m | m | [28] 7.2.2 | c1 | c1 |
| 5 | Authorization | [26] 20.7 | m | m | [26] 20.7 | i | i |
| 6 | Call-ID | [26] 20.8 | m | m | [26] 20.8 | m | m |
| 6A | Contact | [26] 20.10 | m | m | [26] 20.10 | i | i |
| 7 | Content-Disposition | [26] 20.11 | m | m | [26] 20.11 | i | i |
| 8 | Content-Encoding | [26] 20.12 | m | m | [26] 20.12 | i | i |
| 9 | Content-Language | [26] 20.13 | m | m | [26] 20.13 | i | i |
| 10 | Content-Length | [26] 20.14 | m | m | [26] 20.14 | m | m |
| 11 | Content-Type | [26] 20.15 | m | m | [26] 20.15 | i | i |
| 12 | Cseq | [26] 20.16 | m | m | [26] 20.16 | m | m |
| 13 | Date | [26] 20.17 | m | m | [26] 20.17 | c2 | c2 |
| 14 | Event | [28] 7.2.1 | m | m | [28] 7.2.1 | m | m |
| 15 | From | [26] 20.20 | m | m | [26] 20.20 | m | m |
| 16 | Max-Forwards | [26] 20.22 | m | m | [26] 20.22 | m | m |
| 17 | MIME-Version | [26] 20.24 | m | m | [26] 20.24 | i | i |
| 17A | P-Access-Network-Info | [52] 4.4 | c16 | c16 | [52] 4.4 | c17 | c17 |
| 17B | P-Asserted-Identity | [34] 9.1 | c8 | c8 | [34] 9.1 | c9 | c9 |
| 17C | P-Charging-Function-Addresses | [52] 4.5 | c14 | c14 | [52] 4.5 | c15 | c15 |
| 17D | P-Charging-Vector | [52] 4.6 | c12 | n/a | [52] 4.6 | c13 | n/a |
| 17E | P-Preferred-Identity | [34] 9.2 | x | x | [34] 9.2 | c3 | n/a |
| 17F | Privacy | [33] 4.2 | c10 | c10 | [33] 4.2 | c11 | c11 |
| 18 | Proxy-Authorization | [26] 20.28 | m | m | [26] 20.28 | c4 | c4 |
| 19 | Proxy-Require | [26] 20.29 | m | m | [26] 20.29 | m | m |
| 19A | Reason | [34A] 2 | c19 | c19 | [34A] 2 | c20 | c20 |
| 20 | Record-Route | [26] 20.30 | m | m | [26] 20.30 | c7 | c7 |
| 20A | Referred-By | [59] 3 | c23 | c23 | [59] 3 | c24 | c24 |
| 20B | Reject-Contact | [56B] 9.2 | c21 | c21 | [56B] 9.2 | c22 | c22 |
| 20C | Request-Disposition | [56B] 9.1 | c21 | c21 | [56B] 9.1 | c22 | c22 |
| 21 | Require | [26] 20.32 | m | m | [26] 20.32 | c5 | c5 |
| 22 | Route | [26] 20.34 | m | m | [26] 20.34 | m | m |
| 22A | Security-Client | [48] 2.3.1 | x | x | [48] 2.3.1 | c18 | c18 |
| 22B | Security-Verify | [48] 2.3.1 | x | x | [48] 2.3.1 | c18 | c18 |
| 23 | Subscription-State | [28] 8.2.3 | m | m | [28] 8.2.3 | i | i |
| 24 | Supported | [26] 20.37 | m | m | [26] 20.37 | c6 | c6 |
| 25 | Timestamp | [26] 20.38 | m | m | [26] 20.38 | i | i |
| 26 | To | [26] 20.39 | m | m | [26] 20.39 | m | m |
| 27 | User-Agent | [26] 20.41 | m | m | [26] 20.41 | i | i |
| 28 | Via | [26] 20.42 | m | m | [26] 20.42 | m | m |
| 29 | Warning | [26] 20.43 | m | m | [26] 20.43 | i | i |

| | |
|---|---|
| c1: | IF A.4/20 THEN m ELSE i - - SIP specific event notification extension. |
| c2: | IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses. |
| c3: | IF A.162/30A THEN m ELSE n/a - - act as first entity within the trust domain for asserted identity. |
| c4: | IF A.162/8A THEN m ELSE i - - authentication between UA and proxy. |
| c5: | IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER. |
| c6: | IF A.162/16 THEN m ELSE i - - reading the contents of the Supported header before proxying the response. |
| c7: | IF A.162/14 THEN (IF A.162/22 OR A.162/27 THEN m ELSE o) ELSE i - - the requirement to be able to insert itself in the subsequent transactions in a dialog or (the REFER method or SIP specific event notification). |
| c8: | IF A.162/30 THEN m ELSE n/a - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks. |
| c9: | IF A.162/30A or A.162/30B THEN m ELSE i - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks or subsequent entity within trust network that can route outside the trust network. |
| c10: | IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP). |
| c11: | IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently. |
| c12: | IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension. |
| c13: | IF A.162/46 THEN m ELSE IF A.162/45 THEN i ELSE n/a - - adding, deleting, reading or modifying the P-Charging-Vector header before proxying the request or response or the P-Charging-Vector header extension. |
| c14: | IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension. |
| c15: | IF A.162/44A THEN m ELSE IF A.162/44 THEN i ELSE n/a - - adding, deleting or reading the P-Charging-Function-Addresses header before proxying the request or response, or the P-Charging-Function-Addresses header extension. |
| c16: | IF A.162/43 THEN x ELSE IF A.162/41 THEN m ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension. |
| c17: | IF A.162/43 THEN m ELSE IF A.162/41 THEN i ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension. |
| c18: | IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. |
| c19: | IF A.162/48 THEN m ELSE n/a - - the Reason header field for the session initiation protocol. |
| c20: | IF A.162/48 THEN i ELSE n/a - - the Reason header field for the session initiation protocol. |
| c21: | IF A.162/50 THEN m ELSE n/a - - caller preferences for the session initiation protocol. |
| c22: | IF A.162/50 THEN i ELSE n/a - - caller preferences for the session initiation protocol. |
| c23: | IF A.162/53 THEN i ELSE n/a - - the SIP Referred-By mechanism. |
| c24: | IF A.162/53 THEN m ELSE n/a - - the SIP Referred-By mechanism. |
| NOTE: | c1 refers to the UA role major capability as this is the case of a proxy that also acts as a UA specifically for SUBSCRIBE and NOTIFY. |

Prerequisite A.163/10 - - NOTIFY request

**Table A.220: Supported message bodies within the NOTIFY request**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | sipfrag | [37] 2 | m | m | [37] 2 | i | i |

Prerequisite A.163/11 - - NOTIFY response for all status-codes

**Table A.221: Supported headers within the NOTIFY response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 0A | Allow | [26] 20.5 | m | m | [26] 20.5 | i | i |
| 1 | Call-ID | [26] 20.8 | m | m | [26] 20.8 | m | m |
| 2 | Content-Disposition | [26] 20.11 | m | m | [26] 20.11 | i | i |
| 3 | Content-Encoding | [26] 20.12 | m | m | [26] 20.12 | i | i |
| 4 | Content-Language | [26] 20.13 | m | m | [26] 20.13 | i | i |
| 5 | Content-Length | [26] 20.14 | m | m | [26] 20.14 | m | m |
| 6 | Content-Type | [26] 20.15 | m | m | [26] 20.15 | i | i |
| 7 | Cseq | [26] 20.16 | m | m | [26] 20.16 | m | m |
| 8 | Date | [26] 20.17 | m | m | [26] 20.17 | c1 | c1 |
| 9 | From | [26] 20.20 | m | m | [26] 20.20 | m | m |
| 10 | MIME-Version | [26] 20.24 | m | m | [26] 20.24 | i | i |
| 10A | P-Access-Network-Info | [52] 4.4 | c11 | c11 | [52] 4.4 | c12 | c12 |
| 10B | P-Asserted-Identity | [34] 9.1 | c3 | c3 | [34] 9.1 | c4 | c4 |
| 10C | P-Charging-Function-Addresses | [52] 4.5 | c9 | c9 | [52] 4.5 | c10 | c10 |
| 10D | P-Charging-Vector | [52] 4.6 | c7 | n/a | [52] 4.6 | c8 | n/a |
| 10E | P-Preferred-Identity | [34] 9.2 | x | x | [34] 9.2 | c2 | n/a |
| 10F | Privacy | [33] 4.2 | c5 | c5 | [33] 4.2 | c6 | c6 |
| 10G | Require | [26] 20.32 | m | m | [26] 20.32 | c13 | c13 |
| 10H | Server | [26] 20.35 | m | m | [26] 20.35 | i | i |
| 11 | Timestamp | [26] 20.38 | m | m | [26] 20.38 | i | i |
| 12 | To | [26] 20.39 | m | m | [26] 20.39 | m | m |
| 12A | User-Agent | [26] 20.41 | m | m | [26] 20.41 | i | i |
| 13 | Via | [26] 20.42 | m | m | [26] 20.42 | m | m |
| 14 | Warning | [26] 20.43 | m | m | [26] 20.43 | i | i |
| c1: | IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses. | | | | | | |
| c2: | IF A.162/30A THEN m ELSE n/a - - act as first entity within the trust domain for asserted identity. | | | | | | |
| c3: | IF A.162/30 THEN m ELSE n/a - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks. | | | | | | |
| c4: | IF A.162/30A or A.162/30B THEN m ELSE i - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks or subsequent entity within trust network that can route outside the trust network. | | | | | | |
| c5: | IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP). | | | | | | |
| c6: | IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently. | | | | | | |
| c7: | IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension. | | | | | | |
| c8: | IF A.162/46 THEN m ELSE IF A.162/45 THEN i ELSE n/a - - adding, deleting, reading or modifying the P-Charging-Vector header before proxying the request or response or the P-Charging-Vector header extension. | | | | | | |
| c9: | IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension. | | | | | | |
| c10: | IF A.162/44A THEN m ELSE IF A.162/44 THEN i ELSE n/a - - adding, deleting or reading the P-Charging-Function-Addresses header before proxying the request or response, or the P-Charging-Function-Addresses header extension. | | | | | | |
| c11: | IF A.162/43 THEN x ELSE IF A.162/41 THEN m ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension. | | | | | | |
| c12: | IF A.162/43 THEN m ELSE IF A.162/41 THEN i ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension. | | | | | | |
| c13: | IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER. | | | | | | |

Prerequisite A.163/11 - - NOTIFY response

Prerequisite: A.164/102 - - Additional for 2xx response

**Table A.222: Supported headers within the NOTIFY response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 0A | Allow-Events | [28] 7.2.2 | m | m | [28] 7.2.2 | c1 | c1 |
| 1 | Authentication-Info | [26] 20.6 | m | m | [26] 20.6 | i | i |
| 1A | Contact | [26] 20.10 | m | m | [26] 20.10 | i | i |
| 2 | Record-Route | [26] 20.30 | m | m | [26] 20.30 | c3 | c3 |
| 5 | Supported | [26] 20.37 | m | m | [26] 20.37 | i | i |
| c1: | IF A.4/20 THEN m ELSE i - - SIP specific event notification extension. | | | | | | |
| c3: | IF A.162/15 THEN m ELSE i - - the requirement to be able to use separate URIs in the upstream direction and downstream direction when record routeing. | | | | | | |

Prerequisite A.163/11 - - NOTIFY response

Prerequisite: A.164/103 OR A.164/104 OR A.164/105 OR A.164/106 - - Additional for 3xx – 6xx response

**Table A.222A: Supported headers within the NOTIFY response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Error-Info | [26] 20.18 | m | m | [26] 20.18 | i | i |

Prerequisite A.163/11 - - NOTIFY response

Prerequisite: A.164/103 - - Additional for 3xx response

**Table A.223: Supported headers within the NOTIFY response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Contact | [26] 20.10 | m | m | [26] 20.10 | c1 | c1 |
| c1: | IF A.162/19E THEN m ELSE i - - deleting Contact headers. | | | | | | |

Prerequisite A.163/11 - - NOTIFY response

Prerequisite: A.164/14 - - Additional for 401 (Unauthorized) response

**Table A.224: Supported headers within the NOTIFY response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 2 | Proxy-Authenticate | [26] 20.27 | m | m | [26] 20.27 | m | m |
| 8 | WWW-Authenticate | [26] 20.44 | m | m | [26] 20.44 | i | i |

Prerequisite A.163/11 - - NOTIFY response

Prerequisite: A.164/17 OR A.164/23 OR A.164/30 OR A.164/36 OR A.164/42 OR A.164/45 OR A.164/50 OR A.164/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response

**Table A.225: Supported headers within the NOTIFY response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 3 | Retry-After | [26] 20.33 | m | m | [26] 20.33 | i | i |

**Table A.226: Void**

Prerequisite A.163/11 - - NOTIFY response

Prerequisite: A.164/20 - - Additional for 407 (Proxy Authentication Required) response

**Table A.227: Supported headers within the NOTIFY response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 2 | Proxy-Authenticate | [26] 20.27 | m | m | [26] 20.27 | m | m |
| 6 | WWW-Authenticate | [26] 20.44 | m | m | [26] 20.44 | i | i |

Prerequisite A.163/11 - - NOTIFY response

Prerequisite: A.164/25 - - Additional for 415 (Unsupported Media Type) response

**Table A.228: Supported headers within the NOTIFY response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Accept | [26] 20.1 | m | m | [26] 20.1 | i | i |
| 2 | Accept-Encoding | [26] 20.2 | m | m | [26] 20.2 | i | i |
| 3 | Accept-Language | [26] 20.3 | m | m | [26] 20.3 | i | i |

Prerequisite A.163/11 - - NOTIFY response

Prerequisite: A.164/27 - - Additional for 420 (Bad Extension) response

**Table A.229: Supported headers within the NOTIFY response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 5 | Unsupported | [26] 20.40 | m | m | [26] 20.40 | c3 | c3 |
| c3: | IF A.162/18 THEN m ELSE i - - reading the contents of the Unsupported header before proxying the 420 response to a method other than REGISTER. | | | | | | |

Prerequisite A.163/11 - - NOTIFY response

Prerequisite: A.164/28 OR A.164/41A - - Additional for 421 (Extension Required), 494 (Security Agreement Required) response

**Table A.229A: Supported headers within the NOTIFY response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 3 | Security-Server | [48] 2 | c1 | c1 | [48] 2 | n/a | n/a |
| c1: | IF A.162/47 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. | | | | | | |

**Table A.230: Void**

Prerequisite A.163/11 - - NOTIFY response

Prerequisite: A.164/35 - - Additional for 485 (Ambigious) response

**Table A.230A: Supported headers within the NOTIFY response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Contact | [26] 20.10 | m | m | [26] 20.10 | i | i |

Prerequisite A.163/11 - - NOTIFY response

Prerequisite: A.164/39 - - Additional for 489 (Bad Event) response

**Table A.231: Supported headers within the NOTIFY response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Allow-Events | [28] 7.2.2 | m | m | [28] 7.2.2 | c1 | c1 |
| c1: | IF A.4/20 THEN m ELSE i - - SIP specific event notification extension. | | | | | | |
| NOTE: | c1 refers to the UA role major capability as this is the case of a proxy that also acts as a UA specifically for SUBSCRIBE and NOTIFY. | | | | | | |

Prerequisite A.163/11 - - NOTIFY response

**Table A.232: Supported message bodies within the NOTIFY response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | | | | | | | |

### A.2.2.4.9 OPTIONS method

Prerequisite A.163/12 - - OPTIONS request

**Table A.233: Supported headers within the OPTIONS request**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Accept | [26] 20.1 | m | m | [26] 20.1 | i | i |
| 1A | Accept-Contact | [56B] 9.2 | c28 | c28 | [56B] 9.2 | c28 | c29 |
| 2 | Accept-Encoding | [26] 20.2 | m | m | [26] 20.2 | i | i |
| 3 | Accept-Language | [26] 20.3 | m | m | [26] 20.3 | i | i |
| 3A | Allow | [26] 20.5 | m | m | [26] 20.5 | i | i |
| 4 | Allow-Events | [28] 7.2.2 | m | m | [28] 7.2.2 | c1 | c1 |
| 5 | Authorization | [26] 20.7 | m | m | [26] 20.7 | i | i |
| 6 | Call-ID | [26] 20.8 | m | m | [26] 20.8 | m | m |
| 7 | Call-Info | [26] 20.9 | m | m | [26] 20.9 | c4 | c4 |
| 8 | Contact | [26] 20.10 | m | m | [26] 20.10 | i | i |
| 9 | Content-Disposition | [26] 20.11 | m | m | [26] 20.11 | i | i |
| 10 | Content-Encoding | [26] 20.12 | m | m | [26] 20.12 | i | i |
| 11 | Content-Language | [26] 20.13 | m | m | [26] 20.13 | i | i |
| 12 | Content-Length | [26] 20.14 | m | m | [26] 20.14 | m | m |
| 13 | Content-Type | [26] 20.15 | m | m | [26] 20.15 | i | i |
| 14 | Cseq | [26] 20.16 | m | m | [26] 20.16 | m | m |
| 15 | Date | [26] 20.17 | m | m | [26] 20.17 | c2 | c2 |
| 16 | From | [26] 20.20 | m | m | [26] 20.20 | m | m |
| 17 | Max-Forwards | [26] 20.22 | m | m | [26] 20.22 | m | m |
| 18 | MIME-Version | [26] 20.24 | m | m | [26] 20.24 | i | i |
| 19 | Organization | [26] 20.25 | m | m | [26] 20.25 | c3 | c3 |
| 19A | P-Access-Network-Info | [52] 4.4 | c23 | c23 | [52] 4.4 | c24 | c24 |
| 19B | P-Asserted-Identity | [34] 9.1 | c10 | c10 | [34] 9.1 | c11 | c11 |
| 19C | P-Called-Party-ID | [52] 4.2 | c14 | c14 | [52] 4.2 | c15 | c16 |
| 19D | P-Charging-Function-Addresses | [52] 4.5 | c21 | c21 | [52] 4.5 | c22 | c22 |
| 19E | P-Charging-Vector | [52] 4.6 | c19 | c19 | [52] 4.6 | c20 | c20 |
| 19F | P-Preferred-Identity | [34] 9.2 | x | x | [34] 9.2 | c9 | c9 |
| 19G | P-Visited-Network-ID | [52] 4.3 | c17 | n/a | [52] 4.3 | c18 | n/a |
| 19H | Privacy | [33] 4.2 | c12 | c12 | [33] 4.2 | c13 | c13 |
| 20 | Proxy-Authorization | [26] 20.28 | m | m | [26] 20.28 | c8 | c8 |
| 21 | Proxy-Require | [26] 20.29 | m | m | [26] 20.29 | m | m |
| 21A | Reason | [34A] 2 | c26 | c26 | [34A] 2 | c27 | c27 |
| 22 | Record-Route | [26] 20.30 | m | m | [26] 20.30 | c7 | c7 |
| 22A | Referred-By | [59] 3 | c30 | c30 | [59] 3 | c31 | c31 |
| 22B | Reject-Contact | [56B] 9.2 | c28 | c28 | [56B] 9.2 | c28 | c29 |
| 22C | Request-Disposition | [56B] 9.1 | c28 | c28 | [56B] 9.1 | c28 | c28 |
| 23 | Require | [26] 20.32 | m | m | [26] 20.32 | c5 | c5 |
| 24 | Route | [26] 20.34 | m | m | [26] 20.34 | m | m |
| 24A | Security-Client | [48] 2.3.1 | x | x | [48] 2.3.1 | c25 | c25 |
| 24B | Security-Verify | [48] 2.3.1 | x | x | [48] 2.3.1 | c25 | c25 |
| 25 | Supported | [26] 20.37 | m | m | [26] 20.37 | c6 | c6 |
| 26 | Timestamp | [26] 20.38 | m | m | [26] 20.38 | i | i |
| 27 | To | [26] 20.39 | m | m | [26] 20.39 | m | m |
| 28 | User-Agent | [26] 20.41 | m | m | [26] 20.41 | i | i |
| 29 | Via | [26] 20.42 | m | m | [26] 20.42 | m | m |

| | |
|---|---|
| c1: | IF A.4/20 THEN m ELSE i - - SIP specific event notification extension. |
| c2: | IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses. |
| c3: | IF A.162/19A OR A.162/19B THEN m ELSE i - - reading, adding or concatenating the Organization header. |
| c4: | IF A.162/19C OR A.162/19D THEN m ELSE i - - reading, adding or concatenating the Call-Info header. |
| c5: | IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER. |
| c6: | IF A.162/16 THEN m ELSE i - - reading the contents of the Supported header before proxying the response. |
| c7: | IF A.162/14 THEN o ELSE i - - the requirement to be able to insert itself in the subsequent transactions in a dialog. |
| c8: | IF A.162/8A THEN m ELSE i - - authentication between UA and proxy. |
| c9: | IF A.162/30A THEN m ELSE n/a - - act as first entity within the trust domain for asserted identity. |
| c10: | IF A.162/30 THEN m ELSE n/a - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks. |
| c11: | IF A.162/30A or A.162/30B THEN m ELSE i - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks or subsequent entity within trust network that can route outside the trust network. |
| c12: | IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP). |
| c13: | IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently. |
| c14: | IF A.162/37 THEN m ELSE n/a - - the P-Called-Party-ID header extension. |
| c15: | IF A.162/37 THEN i ELSE n/a - - the P-Called-Party-ID header extension. |
| c16: | IF A.162/37 AND A.3/2 THEN m ELSE IF A.162/37 AND A.3/3 THEN i ELSE n/a - - the P-Called-Party-ID header extension and P-CSCF or I-CSCF. |
| c17: | IF A.162/38 THEN m ELSE n/a - - the P-Visited-Network-ID header extension. |
| c18: | IF A.162/39 THEN m ELSE i - - reading, or deleting the P-Visited-Network-ID header before proxying the request or response. |
| c19: | IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension. |
| c20: | IF A.162/46 THEN m ELSE IF A.162/45 THEN i ELSE n/a - - adding, deleting, reading or modifying the P-Charging-Vector header before proxying the request or response or the P-Charging-Vector header extension. |
| c21: | IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension. |
| c22: | IF A.162/44A THEN m ELSE IF A.162/44 THEN i ELSE n/a - - adding, deleting or reading the P-Charging-Function-Addresses header before proxying the request or response, or the P-Charging-Function-Addresses header extension. |
| c23: | IF A.162/43 THEN x ELSE IF A.162/41 THEN m ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension. |
| c24: | IF A.162/43 THEN m ELSE IF A.162/41 THEN i ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension. |
| c25: | IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. |
| c26: | IF A.162/48 THEN m ELSE n/a - - the Reason header field for the session initiation protocol. |
| c27: | IF A.162/48 THEN i ELSE n/a - - the Reason header field for the session initiation protocol. |
| c28: | IF A.162/50 THEN m ELSE n/a - - caller preferences for the session initiation protocol. |
| c29: | IF A.162/50 AND A.4/3 THEN m ELSE IF A.162/50 AND NOT A.4/3 THEN i ELSE n/a - - caller preferences for the session initiation protocol, and S-CSCF. |
| c30: | IF A.162/53 THEN i ELSE n/a - - the SIP Referred-By mechanism. |
| c31: | IF A.162/53 THEN m ELSE n/a - - the SIP Referred-By mechanism. |
| NOTE: | c1 refers to the UA role major capability as this is the case of a proxy that also acts as a UA specifically for SUBSCRIBE and NOTIFY. |

Prerequisite A.163/12 - - OPTIONS request

**Table A.234: Supported message bodies within the OPTIONS request**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | | | | | | | |

**Table A.235: Void**

Prerequisite A.163/13 - - OPTIONS response for all status-codes

**Table A.236: Supported headers within the OPTIONS response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 0A | Allow | [26] 20.5 | m | m | [26] 20.5 | i | i |
| 1 | Call-ID | [26] 20.8 | m | m | [26] 20.8 | m | m |
| 1A | Call-Info | [26] 20.9 | m | m | [26] 20.9 | c3 | c3 |
| 2 | Content-Disposition | [26] 20.11 | m | m | [26] 20.11 | i | i |
| 3 | Content-Encoding | [26] 20.12 | m | m | [26] 20.12 | i | i |
| 4 | Content-Language | [26] 20.13 | m | m | [26] 20.13 | i | i |
| 5 | Content-Length | [26] 20.14 | m | m | [26] 20.14 | m | m |
| 6 | Content-Type | [26] 20.15 | m | m | [26] 20.15 | i | i |
| 7 | Cseq | [26] 20.16 | m | m | [26] 20.16 | m | m |
| 8 | Date | [26] 20.17 | m | m | [26] 20.17 | c1 | c1 |
| 9 | From | [26] 20.20 | m | m | [26] 20.20 | m | m |
| 10 | MIME-Version | [26] 20.24 | m | m | [26] 20.24 | i | i |
| 11 | Organization | [26] 20.25 | m | m | [26] 20.25 | c2 | c2 |
| 11A | P-Access-Network-Info | [52] 4.4 | c13 | c13 | [52] 4.4 | c14 | c14 |
| 11B | P-Asserted-Identity | [34] 9.1 | c5 | c5 | [34] 9.1 | c6 | c6 |
| 11C | P-Charging-Function-Addresses | [52] 4.5 | c11 | c11 | [52] 4.5 | c12 | c12 |
| 11D | P-Charging-Vector | [52] 4.6 | c9 | c9 | [52] 4.6 | c10 | c10 |
| 11E | P-Preferred-Identity | [34] 9.2 | x | x | [34] 9.2 | c4 | n/a |
| 11F | Privacy | [33] 4.2 | c7 | c7 | [33] 4.2 | c8 | c8 |
| 11G | Require | [26] 20.32 | m | m | [26] 20.32 | c15 | c15 |
| 11H | Server | [26] 20.35 | m | m | [26] 20.35 | i | i |
| 12 | Timestamp | [26] 20.38 | m | m | [26] 20.38 | i | i |
| 13 | To | [26] 20.39 | m | m | [26] 20.39 | m | m |
| 13A | User-Agent | [26] 20.41 | m | m | [26] 20.41 | i | i |
| 14 | Via | [26] 20.42 | m | m | [26] 20.42 | m | m |
| 15 | Warning | [26] 20.43 | m | m | [26] 20.43 | i | i |

c1: IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses.
c2: IF A.162/19A OR A.162/19B THEN m ELSE i - - reading, adding or concatenating the Organization header.
c3: IF A.162/19C OR A.162/19D THEN m ELSE i - - reading, adding or concatenating the Call-Info header.
c4: IF A.162/30A THEN m ELSE n/a - - act as first entity within the trust domain for asserted identity.
c5: IF A.162/30 THEN m ELSE n/a - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.
c6: IF A.162/30A or A.162/30B THEN m ELSE i - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks or subsequent entity within trust network that can route outside the trust network.
c7: IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c8: IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently.
c9: IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.
c10: IF A.162/46 THEN m ELSE IF A.162/45 THEN i ELSE n/a - - adding, deleting, reading or modifying the P-Charging-Vector header before proxying the request or response or the P-Charging-Vector header extension.
c11: IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.
c12: IF A.162/44A THEN m ELSE IF A.162/44 THEN i ELSE n/a - - adding, deleting or reading the P-Charging-Function-Addresses header before proxying the request or response, or the P-Charging-Function-Addresses header extension.
c13: IF A.162/43 THEN x ELSE IF A.162/41 THEN m ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.
c14: IF A.162/43 THEN m ELSE IF A.162/41 THEN i ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.
c15: IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER.

Prerequisite A.163/13 - - OPTIONS response

Prerequisite: A.164/102 - - Additional for 2xx response

**Table A.237: Supported headers within the OPTIONS response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Accept | [26] 20.1 | m | m | [26] 20.1 | i | i |
| 1A | Accept-Encoding | [26] 20.2 | m | m | [26] 20.2 | i | i |
| 1B | Accept-Language | [26] 20.3 | m | m | [26] 20.3 | i | i |
| 2 | Allow-Events | [28] 7.2.2 | m | m | [28] 7.2.2 | c1 | c1 |
| 3 | Authentication-Info | [26] 20.6 | m | m | [26] 20.6 | i | i |
| 5 | Contact | [26] 20.10 | m | m | [26] 20.10 | i | i |
| 9 | Record-Route | [26] 20.30 | m | m | [26] 20.30 | c3 | c3 |
| 12 | Supported | [26] 20.37 | m | m | [26] 20.37 | i | i |
| c1: | IF A.4/20 THEN m ELSE i - - SIP specific event notification extension. | | | | | | |
| c3: | IF A.162/15 THEN o ELSE i - - the requirement to be able to use separate URIs in the upstream direction and downstream direction when record routeing. | | | | | | |

Prerequisite A.163/13 - - OPTIONS response

Prerequisite: A.164/103 OR A.164/104 OR A.164/105 OR A.164/106 - - Additional for 3xx – 6xx response

**Table A.237A: Supported headers within the OPTIONS response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Error-Info | [26] 20.18 | m | m | [26] 20.18 | i | i |

Prerequisite A.163/13 - - OPTIONS response

Prerequisite: A.164/103 OR A.164/35 - - Additional for 3xx or 485 (Ambiguous) response

**Table A.238: Supported headers within the OPTIONS response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 3 | Contact | [26] 20.10 | m | m | [26] 20.10 | c1 | c1 |
| c1: | IF A.162/19E THEN m ELSE i - - deleting Contact headers. | | | | | | |

Prerequisite A.163/13 - - OPTIONS response

Prerequisite: A.164/14 - - Additional for 401 (Unauthorized) response

**Table A.239: Supported headers within the OPTIONS response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 4 | Proxy-Authenticate | [26] 20.27 | m | m | [26] 20.27 | m | m |
| 10 | WWW-Authenticate | [26] 20.44 | m | m | [26] 20.44 | i | i |

Prerequisite A.163/13 - - OPTIONS response

Prerequisite: A.164/17 OR A.164/23 OR A.164/30 OR A.164/36 OR A.164/42 OR A.164/45 OR A.164/50 OR A.164/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response

**Table A.240: Supported headers within the OPTIONS response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 5 | Retry-After | [26] 20.33 | m | m | [26] 20.33 | i | i |

**Table A.241: Void**

Prerequisite A.163/13 - - OPTIONS response

Prerequisite: A.164/20 - - Additional for 407 (Proxy Authentication Required) response

**Table A.242: Supported headers within the OPTIONS response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 4 | Proxy-Authenticate | [26] 20.27 | m | m | [26] 20.27 | m | m |
| 8 | WWW-Authenticate | [26] 20.44 | m | m | [26] 20.44 | i | i |

Prerequisite A.163/13 - - OPTIONS response

Prerequisite: A.164/25 - - Additional for 415 (Unsupported Media Type) response

**Table A.243: Supported headers within the OPTIONS response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Accept | [26] 20.1 | m | m | [26] 20.1 | i | i |
| 2 | Accept-Encoding | [26] 20.2 | m | m | [26] 20.2 | i | i |
| 3 | Accept-Language | [26] 20.3 | m | m | [26] 20.3 | i | i |

Prerequisite A.163/13 - - OPTIONS response

Prerequisite: A.164/27 - - Additional for 420 (Bad Extension) response

**Table A.244: Supported headers within the OPTIONS response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 7 | Unsupported | [26] 20.40 | m | m | [26] 20.40 | c3 | c3 |
| c3: | IF A.162/18 THEN m ELSE i - - reading the contents of the Unsupported header before proxying the 420 response to a method other than REGISTER. | | | | | | |

Prerequisite A.163/13 - - OPTIONS response

Prerequisite: A.164/28 OR A.164/41A - - Additional for 421 (Extension Required), 494 (Security Agreement Required) response

**Table A.244A: Supported headers within the OPTIONS response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 3 | Security-Server | [48] 2 | c1 | c1 | [48] 2 | n/a | n/a |
| c1: | IF A.162/47 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. | | | | | | |

**Table A.245: Void**

Prerequisite A.163/13 - - OPTIONS response

**Table A.246: Supported message bodies within the OPTIONS response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | | | | | | | |

### A.2.2.4.10 PRACK method

Prerequisite A.163/14 - - PRACK request

**Table A.247: Supported headers within the PRACK request**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Accept | [26] 20.1 | m | m | [26] 20.1 | i | i |
| 1A | Accept-Contact | [56B] 9.2 | c18 | c18 | [56B] 9.2 | c19 | c19 |
| 2 | Accept-Encoding | [26] 20.2 | m | m | [26] 20.2 | i | i |
| 3 | Accept-Language | [26] 20.3 | m | m | [26] 20.3 | i | i |
| 3A | Allow | [26] 20.5 | m | m | [26] 20.5 | i | i |
| 4 | Allow-Events | [28] 7.2.2 | m | m | [28] 7.2.2 | c1 | c1 |
| 5 | Authorization | [26] 20.7 | m | m | [26] 20.7 | i | i |
| 6 | Call-ID | [26] 20.8 | m | m | [26] 20.8 | m | m |
| 7 | Content-Disposition | [26] 20.11 | m | m | [26] 20.11 | i | c3 |
| 8 | Content-Encoding | [26] 20.12 | m | m | [26] 20.12 | i | c3 |
| 9 | Content-Language | [26] 20.13 | m | m | [26] 20.13 | i | c3 |
| 10 | Content-Length | [26] 20.14 | m | m | [26] 20.14 | m | m |
| 11 | Content-Type | [26] 20.15 | m | m | [26] 20.15 | i | c3 |
| 12 | Cseq | [26] 20.16 | m | m | [26] 20.16 | m | m |
| 13 | Date | [26] 20.17 | m | m | [26] 20.17 | c2 | c2 |
| 14 | From | [26] 20.20 | m | m | [26] 20.20 | m | m |
| 15 | Max-Forwards | [26] 20.22 | m | m | [26] 20.22 | m | m |
| 16 | MIME-Version | [26] 20.24 | m | m | [26] 20.24 | i | c3 |
| 16A | P-Access-Network-Info | [52] 4.4 | c14 | c14 | [52] 4.4 | c15 | c15 |
| 16B | P-Charging-Function-Addresses | [52] 4.5 | c12 | c12 | [52] 4.5 | c13 | c13 |
| 16C | P-Charging-Vector | [52] 4.6 | c10 | n/a | [52] 4.6 | c11 | n/a |
| 16D | Privacy | [33] 4.2 | c8 | c8 | [33] 4.2 | c9 | c9 |
| 17 | Proxy-Authorization | [26] 20.28 | m | m | [26] 20.28 | c4 | c4 |
| 18 | Proxy-Require | [26] 20.29 | m | m | [26] 20.29 | m | m |
| 19 | Rack | [27] 7.2 | m | m | [27] 7.2 | i | i |
| 19A | Reason | [34A] 2 | c16 | c16 | [34A] 2 | c17 | c17 |
| 20 | Record-Route | [26] 20.30 | m | m | [26] 20.30 | c7 | c7 |
| 20A | Referred-By | [59] 3 | c20 | c20 | [59] 3 | c21 | c21 |
| 20B | Reject-Contact | [56B] 9.2 | c18 | c18 | [56B] 9.2 | c19 | c19 |
| 20C | Request-Disposition | [56B] 9.1 | c18 | c18 | [56B] 9.1 | c19 | c19 |
| 21 | Require | [26] 20.32 | m | m | [26] 20.32 | c5 | c5 |
| 22 | Route | [26] 20.34 | m | m | [26] 20.34 | m | m |
| 23 | Supported | [26] 20.37 | m | m | [26] 20.37 | c6 | c6 |
| 24 | Timestamp | [26] 20.38 | m | m | [26] 20.38 | i | i |
| 25 | To | [26] 20.39 | m | m | [26] 20.39 | m | m |
| 26 | User-Agent | [26] 20.41 | m | m | [26] 20.41 | i | i |
| 27 | Via | [26] 20.42 | m | m | [26] 20.42 | m | m |

| | |
|---|---|
| c1: | IF A.4/20 THEN m ELSE i - - SIP specific event notification extension. |
| c2: | IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses. |
| c3: | IF A.3/2 OR A.3/4 THEN m ELSE i - - P-CSCF or S-CSCF. |
| c4: | IF A.162/8A THEN m ELSE i - - authentication between UA and proxy. |
| c5: | IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER. |
| c6: | IF A.162/16 THEN m ELSE i - - reading the contents of the Supported header before proxying the response. |
| c7: | IF A.162/14 THEN 0 ELSE i - - the requirement to be able to insert itself in the subsequent transactions in a dialog. |
| c8: | IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP). |
| c9: | IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently. |
| c10: | IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension. |
| c11: | IF A.162/46 THEN m ELSE IF A.162/45 THEN i ELSE n/a - - adding, deleting, reading or modifying the P-Charging-Vector header before proxying the request or response or the P-Charging-Vector header extension. |
| c12: | IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension. |
| c13: | IF A.162/44A THEN m ELSE IF A.162/44 THEN i ELSE n/a - - adding, deleting or reading the P-Charging-Function-Addresses header before proxying the request or response, or the P-Charging-Function-Addresses header extension. |
| c14: | IF A.162/43 THEN x ELSE IF A.162/41 THEN m ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension. |
| c15: | IF A.162/43 THEN m ELSE IF A.162/41 THEN i ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension. |
| c16: | IF A.162/48 THEN m ELSE n/a - - the Reason header field for the session initiation protocol. |
| c17: | IF A.162/48 THEN i ELSE n/a - - the Reason header field for the session initiation protocol. |
| c18: | IF A.162/50 THEN m ELSE n/a - - caller preferences for the session initiation protocol. |
| c19: | IF A.162/50 THEN i ELSE n/a - - caller preferences for the session initiation protocol. |
| c20: | IF A.162/53 THEN i ELSE n/a - - the SIP Referred-By mechanism. |
| c21: | IF A.162/53 THEN m ELSE n/a - - the SIP Referred-By mechanism. |
| NOTE: | c1 refers to the UA role major capability as this is the case of a proxy that also acts as a UA specifically for SUBSCRIBE and NOTIFY. |

Prerequisite A.163/14 - - PRACK request

**Table A.248: Supported message bodies within the PRACK request**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | | | | | | | |

**Table A.249: Void**

Prerequisite A.163/15 - - PRACK response for all status-codes

**Table A.250: Supported headers within the PRACK response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 0A | Allow | [26] 20.5 | m | m | [26] 20.5 | i | i |
| 1 | Call-ID | [26] 20.8 | m | m | [26] 20.8 | m | m |
| 2 | Content-Disposition | [26] 20.11 | m | m | [26] 20.11 | i | c2 |
| 3 | Content-Encoding | [26] 20.12 | m | m | [26] 20.12 | i | c2 |
| 4 | Content-Language | [26] 20.13 | m | m | [26] 20.13 | i | c2 |
| 5 | Content-Length | [26] 20.14 | m | m | [26] 20.14 | m | m |
| 6 | Content-Type | [26] 20.15 | m | m | [26] 20.15 | i | c2 |
| 7 | Cseq | [26] 20.16 | m | m | [26] 20.16 | m | m |
| 8 | Date | [26] 20.17 | m | m | [26] 20.17 | c1 | c1 |
| 9 | From | [26] 20.20 | m | m | [26] 20.20 | m | m |
| 10 | MIME-Version | [26] 20.24 | m | m | [26] 20.24 | i | c2 |
| 10A | P-Access-Network-Info | [52] 4.4 | c9 | c9 | [52] 4.4 | c10 | c10 |
| 10B | P-Charging-Function-Addresses | [52] 4.5 | c7 | c7 | [52] 4.5 | c8 | c8 |
| 10C | P-Charging-Vector | [52] 4.6 | c5 | n/a | [52] 4.6 | c6 | n/a |
| 10D | Privacy | [33] 4.2 | c3 | c3 | [33] 4.2 | c4 | c4 |
| 10E | Require | [26] 20.32 | m | m | [26] 20.32 | c11 | c11 |
| 10F | Server | [26] 20.35 | m | m | [26] 20.35 | i | i |
| 11 | Timestamp | [26] 20.38 | m | m | [26] 20.38 | i | i |
| 12 | To | [26] 20.39 | m | m | [26] 20.39 | m | m |
| 12A | User-Agent | [26] 20.41 | m | m | [26] 20.41 | i | i |
| 13 | Via | [26] 20.42 | m | m | [26] 20.42 | m | m |
| 14 | Warning | [26] 20.43 | m | m | [26] 20.43 | i | i |

c1: IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses.
c2: IF A.3/2 OR A.3/4 THEN m ELSE i - - P-CSCF or S-CSCF.
c3: IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c4: IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently.
c5: IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.
c6: IF A.162/46 THEN m ELSE IF A.162/45 THEN i ELSE n/a - - adding, deleting, reading or modifying the P-Charging-Vector header before proxying the request or response or the P-Charging-Vector header extension.
c7: IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.
c8: IF A.162/44A THEN m ELSE IF A.162/44 THEN i ELSE n/a - - adding, deleting or reading the P-Charging-Function-Addresses header before proxying the request or response, or the P-Charging-Function-Addresses header extension.
c9: IF A.162/43 THEN x ELSE IF A.162/41 THEN m ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.
c10: IF A.162/43 THEN m ELSE IF A.162/41 THEN i ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.
c11: IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER.

Prerequisite A.163/15 - - PRACK response

Prerequisite: A.164/102 - - Additional for 2xx response

**Table A.251: Supported headers within the PRACK response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 0A | Allow-Events | [28] 7.2.2 | m | m | [28] 7.2.2 | c1 | c1 |
| 0B | Authentication-Info | [26] 20.6 | m | m | [26] 20.6 | i | i |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1 | Record-Route | [26] 20.30 | m | m | [26] 20.30 | c3 | c3 |
| 4 | Supported | [26] 20.37 | m | m | [26] 20.37 | i | i |
| c1: | IF A.4/20 THEN m ELSE i - - SIP specific event notification extension. | | | | | | |
| c3: | IF A.162/15 THEN o ELSE i - - the requirement to be able to use separate URIs in the upstream direction and downstream direction when record routeing. | | | | | | |

Prerequisite A.163/3 - - PRACK response

Prerequisite: A.164/103 OR A.164/104 OR A.164/105 OR A.164/106 - - Additional for 3xx – 6xx response

**Table A.251A: Supported headers within the PRACK response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Error-Info | [26] 20.18 | m | m | [26] 20.18 | i | i |

Prerequisite A.163/15 - - PRACK response

Prerequisite: A.164/103 OR A.164/35 - - Additional for 3xx or 485 (Ambiguous) response

**Table A.252: Supported headers within the PRACK response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Contact | [26] 20.10 | m | m | [26] 20.10 | c1 | c1 |
| c1: | IF A.162/19E THEN m ELSE i - - deleting Contact headers. | | | | | | |

Prerequisite A.163/15 - - PRACK response

Prerequisite: A.164/14 - - Additional for 401 (Unauthorized) response

**Table A.253: Supported headers within the PRACK response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 2 | Proxy-Authenticate | [26] 20.27 | m | m | [26] 20.27 | m | m |
| 8 | WWW-Authenticate | [26] 20.44 | m | m | [26] 20.44 | i | i |

Prerequisite A.163/15 - - PRACK response

Prerequisite: A.164/17 OR A.164/23 OR A.164/30 OR A.164/36 OR A.164/42 OR A.164/45 OR A.164/50 OR A.164/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response

**Table A.254: Supported headers within the PRACK response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 3 | Retry-After | [26] 20.33 | m | m | [26] 20.33 | i | i |

**Table A.255: Void**

Prerequisite A.163/15 - - PRACK response

Prerequisite: A.164/20 - - Additional for 407 (Proxy Authentication Required) response

**Table A.256: Supported headers within the PRACK response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 2 | Proxy-Authenticate | [26] 20.27 | m | m | [26] 20.27 | m | m |
| 6 | WWW-Authenticate | [26] 20.44 | m | m | [26] 20.44 | i | i |

Prerequisite A.163/15 - - PRACK response

Prerequisite: A.164/25 - - Additional for 415 (Unsupported Media Type) response

**Table A.257: Supported headers within the PRACK response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Accept | [26] 20.1 | m | m | [26] 20.1 | i | i |
| 2 | Accept-Encoding | [26] 20.2 | m | m | [26] 20.2 | i | i |
| 3 | Accept-Language | [26] 20.3 | m | m | [26] 20.3 | i | i |

Prerequisite A.163/15 - - PRACK response

Prerequisite: A.164/27 - - Addition for 420 (Bad Extension) response

**Table A.258: Supported headers within the PRACK response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 5 | Unsupported | [26] 20.40 | m | m | [26] 20.40 | c3 | c3 |
| c3: | IF A.162/18 THEN m ELSE i - - reading the contents of the Unsupported header before proxying the 420 response to a method other than REGISTER. | | | | | | |

Prerequisite A.163/15 - - PRACK response

Prerequisite: A.164/28 OR A.164/41A - - Additional for 421 (Extension Required), 494 (Security Agreement Required) response

**Table A.258A: Supported headers within the PRACK response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 3 | Security-Server | [48] 2 | c1 | c1 | [48] 2 | n/a | n/a |
| c1: | IF A.162/47 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. | | | | | | |

**Table A.259: Void**

Prerequisite A.163/15 - - PRACK response

**Table A.260: Supported message bodies within the PRACK response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | | | | | | | |

## A.2.2.4.10A PUBLISH method

Prerequisite A.163/15A - - PUBLISH request

**Table A.260A: Supported headers within the PUBLISH request**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Accept-Contact | [56B] 9.2 | c28 | c28 | [56B] 9.2 | c28 | c29 |
| 2 | Allow | [26] 20.5 | m | m | [26] 20.5 | i | i |
| 3 | Allow-Events | [28] 7.2.2 | m | m | [28] 7.2.2 | c29 | c29 |
| 4 | Authorization | [26] 20.7 | m | m | [26] 20.7 | i | i |
| 5 | Call-ID | [26] 20.8 | m | m | [26] 20.8 | m | m |
| 6 | Call-Info | [26] 24.9 | m | m | [26] 24.9 | c4 | c4 |
| 7 | Content-Disposition | [26] 20.11 | m | m | [26] 20.11 | i | i |
| 8 | Content-Encoding | [26] 20.12 | m | m | [26] 20.12 | i | i |
| 9 | Content-Language | [26] 20.13 | m | m | [26] 20.13 | i | i |
| 10 | Content-Length | [26] 20.14 | m | m | [26] 20.14 | m | m |
| 11 | Content-Type | [26] 20.15 | m | m | [26] 20.15 | i | i |
| 12 | Cseq | [26] 20.16 | m | m | [26] 20.16 | m | m |
| 13 | Date | [26] 20.17 | m | m | [26] 20.17 | c2 | c2 |
| 14 | Event | [70] 4, 6 | m | m | [70] 4, 6 | m | m |
| 15 | Expires | [26] 20.19, [70] 4, 5, 6 | m | m | [26] 20.19, [70] 4, 5, 6 | i | i |
| 16 | From | [26] 20.20 | m | m | [26] 20.20 | m | m |
| 17 | In-Reply-To | [26] 20.21 | m | m | [26] 20.21 | i | i |
| 18 | Max-Forwards | [26] 20.22 | m | m | [26] 20.22 | m | m |
| 19 | MIME-Version | [26] 20.24 | m | m | [26] 20.24 | i | i |
| 20 | Organization | [26] 20.25 | m | m | [26] 20.25 | c3 | c3 |
| 21 | P-Access-Network-Info | [52] 4.4 | c23 | c23 | [52] 4.4 | c24 | c24 |
| 22 | P-Asserted-Identity | [34] 9.1 | c10 | c10 | [34] 9.1 | c11 | c11 |
| 23 | P-Called-Party-ID | [52] 4.2 | c14 | c14 | [52] 4.2 | c15 | c16 |
| 24 | P-Charging-Function-Addresses | [52] 4.5 | c21 | c21 | [52] 4.5 | c22 | c22 |
| 25 | P-Charging-Vector | [52] 4.6 | c19 | c19 | [52] 4.6 | c20 | c20 |
| 26 | P-Preferred-Identity | [34] 9.2 | x | x | [34] 9.2 | c9 | c9 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 27 | P-Visited-Network-ID | [52] 4.3 | c17 | n/a | [52] 4.3 | c18 | n/a |
| 28 | Priorità | [26] 20.26 | m | m | [26] 20.26 | i | i |
| 29 | Privacy | [33] 4.2 | c12 | c12 | [33] 4.2 | c13 | c13 |
| 30 | Proxy-Authorization | [26] 20.28 | m | m | [26] 20.28 | c7 | c7 |
| 31 | Proxy-Require | [26] 20.29 | m | m | [26] 20.29 | m | m |
| 32 | Reason | [34A] 2 | c8 | c8 | [34A] 2 | c1 | c1 |
| 33 | Referred-By | [59] 3 | c30 | c30 | [59] 3 | c31 | c31 |
| 34 | Reject-Contact | [56B] 9.2 | c27 | c27 | [56B] 9.2 | c27 | c28 |
| 34A | Reply-To | [26] 20.31 | m | m | [26] 20.31 | i | i |
| 35 | Request-Disposition | [56B] 9.1 | c27 | c27 | [56B] 9.1 | c27 | c27 |
| 36 | Require | [26] 20.32 | m | m | [26] 20.32 | c5 | c5 |
| 37 | Route | [26] 20.34 | m | m | [26] 20.34 | m | m |
| 38 | Security-Client | [48] 2.3.1 | x | x | [48] 2.3.1 | c25 | c25 |
| 39 | Security-Verify | [48] 2.3.1 | x | x | [48] 2.3.1 | c26 | c26 |
| 40 | SIP-If-Match | [70] 11.3.2 | m | m | [70] 11.3.2 | i | i |
| 41 | Subject | [26] 20.36 | m | m | [26] 20.36 | i | i |
| 42 | Supported | [26] 20.37 | m | m | [26] 20.37 | c6 | c6 |
| 43 | Timestamp | [26] 20.38 | m | m | [26] 20.38 | i | i |
| 44 | To | [26] 20.39 | m | m | [26] 20.39 | m | m |
| 45 | User-Agent | [26] 20.41 | m | m | [26] 20.41 | i | i |
| 46 | Via | [26] 20.42 | m | m | [26] 20.42 | m | m |

| | |
|---|---|
| c1: | IF A.162/48 THEN i ELSE n/a - - the Reason header field for the session initiation protocol. |
| c2: | IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses. |
| c3: | IF A.162/19A OR A.162/19B THEN m ELSE i - - reading, adding or concatenating the Organization header. |
| c4: | IF A.162/19C OR A.162/19D THEN m ELSE i - - reading, adding or concatenating the Call-Info header. |
| c5: | IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER. |
| c6: | IF A.162/16 THEN m ELSE i - - reading the contents of the Supported header before proxying the response. |
| c7: | IF A.162/8A THEN m ELSE i - - authentication between UA and proxy. |
| c8: | IF A.162/48 THEN m ELSE n/a - - the Reason header field for the session initiation protocol. |
| c9: | IF A.162/30A THEN m ELSE n/a - - act as first entity within the trust domain for asserted identity. |
| c10: | IF A.162/30 THEN m ELSE n/a - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks. |
| c11: | IF A.162/30A or A.162/30B THEN m ELSE i - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks or subsequent entity within trust network that can route outside the trust network. |
| c12: | IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP). |
| c13: | IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently. |
| c14: | IF A.162/37 THEN m ELSE n/a - - the P-Called-Party-ID header extension. |
| c15: | IF A.162/37 THEN i ELSE n/a - - the P-Called-Party-ID header extension. |
| c16: | IF A.162/37 AND A.3/2 THEN m ELSE IF A.162/37 AND A.3/3 THEN i ELSE n/a - - the P-Called-Party-ID header extension and P-CSCF or I-CSCF. |
| c17: | IF A.162/38 THEN m ELSE n/a - - the P-Visited-Network-ID header extension. |
| c18: | IF A.162/39 THEN m ELSE i - - reading, or deleting the P-Visited-Network-ID header before proxying the request or response. |
| c19: | IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension. |
| c20: | IF A.162/46 THEN m ELSE IF A.162/45 THEN i ELSE n/a - - adding, deleting, reading or modifying the P-Charging-Vector header before proxying the request or response or the P-Charging-Vector header extension. |
| c21: | IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension. |
| c22: | IF A.162/44A THEN m ELSE IF A.162/44 THEN i ELSE n/a - - adding, deleting or reading the P-Charging-Function-Addresses header before proxying the request or response, or the P-Charging-Function-Addresses header extension. |
| c23: | IF A.162/43 THEN x ELSE IF A.162/41 THEN m ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension. |
| c24: | IF A.162/43 THEN m ELSE IF A.162/41 THEN i ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension. |
| c25: | IF A.162/47 THEN o ELSE n/a - - security mechanism agreement for the session initiation protocol (note 1). |
| c26: | IF A.162/47 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. |
| c27: | IF A.162/50 THEN m ELSE n/a - - caller preferences for the session initiation protocol. |
| c28: | IF A.162/50 AND A.4/3 THEN m ELSE IF A.162/50 AND NOT A.4/3 THEN i ELSE n/a - - caller preferences for the session initiation protocol, and S-CSCF. |
| c29: | IF A.4/20 THEN m ELSE i - - SIP specific event notification extension (note 2). |
| c30: | IF A.162/53 THEN i ELSE n/a - - the SIP Referred-By mechanism. |
| c31: | IF A.162/53 THEN m ELSE n/a - - the SIP Referred-By mechanism. |
| NOTE 1: | Support of this header in this method is dependent on the security mechanism and the security architecture which is implemented. |
| NOTE 2: | c29 refers to the UA role major capability as this is the case of a proxy that also acts as a UA specifically for SUBSCRIBE and NOTIFY. |

Prerequisite A.163/15A - - PUBLISH request

**Table A.260B: Supported message bodies within the PUBLISH request**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | | | | | | | |

Prerequisite A.163/15B - - PUBLISH response for all status-codes

**Table A.260C: Supported headers within the PUBLISH response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 0A | Allow | [26] 20.5 | m | m | [26] 20.5 | i | i |
| 1 | Call-ID | [26] 20.8 | m | m | [26] 20.8 | m | m |
| 2 | Call-Info | [26] 24.9 | m | m | [26] 24.9 | c3 | c3 |
| 3 | Content-Disposition | [26] 20.11 | m | m | [26] 20.11 | i | i |
| 4 | Content-Encoding | [26] 20.12 | m | m | [26] 20.12 | i | i |
| 5 | Content-Language | [26] 20.13 | m | m | [26] 20.13 | i | i |
| 6 | Content-Length | [26] 20.14 | m | m | [26] 20.14 | m | m |
| 7 | Content-Type | [26] 20.15 | m | m | [26] 20.15 | i | i |
| 8 | Cseq | [26] 20.16 | m | m | [26] 20.16 | m | m |
| 9 | Date | [26] 20.17 | m | m | [26] 20.17 | c1 | c1 |
| 10 | From | [26] 20.20 | m | m | [26] 20.20 | m | m |
| 11 | MIME-Version | [26] 20.24 | m | m | [26] 20.24 | i | i |
| 12 | Organization | [26] 20.25 | m | m | [26] 20.25 | c2 | c2 |
| 13 | P-Access-Network-Info | [52] 4.4 | c13 | c13 | [52] 4.4 | c14 | c14 |
| 14 | P-Asserted-Identity | [34] 9.1 | c5 | c5 | [34] 9.1 | c6 | c6 |
| 15 | P-Charging-Function-Addresses | [52] 4.5 | c11 | c11 | [52] 4.5 | c12 | c12 |
| 16 | P-Charging-Vector | [52] 4.6 | c9 | n/a | [52] 4.6 | c10 | n/a |
| 17 | P-Preferred-Identity | [34] 9.2 | x | x | [34] 9.2 | c4 | n/a |
| 18 | Privacy | [33] 4.2 | c7 | c7 | [33] 4.2 | c8 | c8 |
| 19 | Require | [26] 20.32 | m | m | [26] 20.32 | c15 | c15 |
| 20 | Server | [26] 20.35 | m | m | [26] 20.35 | i | i |
| 21 | Timestamp | [26] 20.38 | m | m | [26] 20.38 | i | i |
| 22 | To | [26] 20.39 | m | m | [26] 20.39 | m | m |
| 23 | User-Agent | [26] 20.41 | m | m | [26] 20.41 | i | i |
| 24 | Via | [26] 20.42 | m | m | [26] 20.42 | m | m |
| 25 | Warning | [26] 20.43 | m | m | [26] 20.43 | i | i |

c1: IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses.
c2: IF A.162/19A OR A.162/19B THEN m ELSE i - - reading, adding or concatenating the Organization header.
c3: IF A.162/19C OR A.162/19D THEN m ELSE i - - reading, adding or concatenating the Call-Info header.
c4: IF A.162/30A THEN m ELSE n/a - - act as first entity within the trust domain for asserted identity.
c5: IF A.162/30 THEN m ELSE n/a - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.
c6: IF A.162/30A or A.162/30B THEN m ELSE i - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks or subsequent entity within trust network that can route outside the trust network.
c7: IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c8: IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently.
c9: IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.
c10: IF A.162/46 THEN m ELSE IF A.162/45 THEN i ELSE n/a - - adding, deleting, reading or modifying the P-Charging-Vector header before proxying the request or response or the P-Charging-Vector header extension.
c11: IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.
c12: IF A.162/44A THEN m ELSE IF A.162/44 THEN i ELSE n/a - - adding, deleting or reading the P-Charging-Function-Addresses header before proxying the request or response, or the P-Charging-Function-Addresses header extension.
c13: IF A.162/43 THEN x ELSE IF A.162/41 THEN m ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.
c14: IF A.162/43 THEN m ELSE IF A.162/41 THEN i ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.
c15: IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER.

Prerequisite A.163/15B - - PUBLISH response

Prerequisite: A.164/7 - - Additional for 200 (OK) response

**Table A.260D: Supported headers within the PUBLISH response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 2 | Authentication-Info | [26] 20.6 | m | m | [26] 20.6 | i | i |
| 3 | Expires | [26] 20.19, [70] 4, 5, 6 | m | m | [26] 20.19, [70] 4, 5, 6 | i | i |
| 4 | SIP-Etag | [70] 11.3.1 | m | m | [70] 11.3.1 | i | i |
| 5 | Supported | [26] 20.37 | m | m | [26] 20.37 | i | i |

Prerequisite A.163/15B - - PUBLISH response

Prerequisite: A.164/103 OR A.164/104 OR A.164/105 OR A.164/106 - - Additional for 3xx – 6xx response

**Table A.260DA: Supported headers within the PUBLISH response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Error-Info | [26] 20.18 | m | m | [26] 20.18 | i | i |

Prerequisite A.163/15B - - PUBLISH response

Prerequisite: A.164/103 OR A.164/35 - - Additional for 3xx or 485 (Ambiguous) response

**Table A.260E: Supported headers within the PUBLISH response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 2 | Contact | [26] 20.10 | m | m | [26] 20.10 | c1 | c1 |
| c1: | IF A.162/19E THEN m ELSE i - - deleting Contact headers. | | | | | | |

Prerequisite A.163/15B - - PUBLISH response

Prerequisite: A.164/8 OR A.164/9 OR A.164/10 OR A.164/11 OR A.164/12 - - Additional for 401 (Unauthorized) response

**Table A.260F: Supported headers within the PUBLISH response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 3 | Proxy-Authenticate | [26] 20.27 | m | m | [26] 20.27 | m | m |
| 5 | WWW-Authenticate | [26] 20.44 | m | m | [26] 20.44 | i | i |

Prerequisite A.163/15B - - PUBLISH response

Prerequisite: A.164/17 OR A.164/23 OR A.164/30 OR A.164/36 OR A.164/42 OR A.164/45 OR A.164/50 OR A.164/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response

**Table A.260G: Supported headers within the PUBLISH response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 3 | Retry-After | [26] 20.33 | m | m | [26] 20.33 | i | i |

**Table A.260H: Void**

Prerequisite A.163/15B - - PUBLISH response

Prerequisite: A.164/20 - - Additional for 407 (Proxy Authentication Required) response

**Table A.260I: Supported headers within the PUBLISH response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 3 | Proxy-Authenticate | [26] 20.27 | m | m | [26] 20.27 | m | m |
| 5 | WWW-Authenticate | [26] 20.44 | m | m | [26] 20.44 | i | i |

Prerequisite A.163/15B - - PUBLISH response

Prerequisite: A.164/25 - - Additional for 415 (Unsupported Media Type) response

**Table A.260J: Supported headers within the PUBLISH response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Accept | [26] 20.1 | m | m | [26] 20.1 | i | i |
| 2 | Accept-Encoding | [26] 20.2 | m | m | [26] 20.2 | i | i |
| 3 | Accept-Language | [26] 20.3 | m | m | [26] 20.3 | i | i |

Prerequisite A.163/15B - - PUBLISH response

Prerequisite: A.164/27 - - Additional for 420 (Bad Extension) response

**Table A.260K: Supported headers within the PUBLISH response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 4 | Unsupported | [26] 20.40 | m | m | [26] 20.40 | c3 | c3 |
| c3: | IF A.162/18 THEN m ELSE i - - reading the contents of the Unsupported header before proxying the 420 response to a method other than REGISTER. | | | | | | |

Prerequisite A.163/15B - - PUBLISH response

Prerequisite: A.164/28 OR A.164/41A - - Additional for 421 (Extension Required), 494 (Security Agreement Required) response

**Table A.260L: Supported headers within the PUBLISH response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 3 | Security-Server | [48] 2 | c1 | c1 | [48] 2 | n/a | n/a |
| c1: | IF A.162/47 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. | | | | | | |

Prerequisite A.163/15B - - PUBLISH response

Prerequisite: A.164/29 - - Additional for 423 (Interval Too Brief) response

**Table A.260M: Supported headers within the PUBLISH response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 3 | Min-Expires | [26] 20.23, [70] 5, 6 | m | m | [26] 20.23, [70] 5, 6 | i | i |

Prerequisite A.163/15B - - PUBLISH response

Prerequisite: A.164/34 - - 484 (Address Incomplete)

**Table A.260N: Void**

Prerequisite A.163/15B - - PUBLISH response

Prerequisite: A.164/39 - - Additional for 489 (Bad Event) response

**Table A.260O: Supported headers within the PUBLISH response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 2 | Allow-Events | [28] 8.2.2 | m | m | [28] 8.2.2 | i | i |

Prerequisite A.163/17 - - PUBLISH response

**Table A.260P: Supported message bodies within the PUBLISH response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | | | | | | | |

### A.2.2.4.11 REFER method

Prerequisite A.163/16 - - REFER request

**Table A.261: Supported headers within the REFER request**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 0A | Accept | [26] 20.1 | m | m | [26] 20.1 | i | i |
| 0B | Accept-Contact | [56B] 9.2 | c27 | c27 | [56B] 9.2 | c27 | c28 |
| 0C | Accept-Encoding | [26] 20.2 | m | m | [26] 20.2 | i | i |
| 1 | Accept-Language | [26] 20.3 | m | m | [26] 20.3 | i | i |
| 1A | Allow | [26] 20.5 | m | m | [26] 20.5 | i | i |
| 2 | Allow-Events | [28] 7.2.2 | m | m | [28] 7.2.2 | c1 | c1 |
| 3 | Authorization | [26] 20.7 | m | m | [26] 20.7 | i | i |
| 4 | Call-ID | [26] 20.8 | m | m | [26] 20.8 | m | m |
| 5 | Contact | [26] 20.10 | m | m | [26] 20.10 | i | i |
| 5A | Content-Disposition | [26] 20.11 | m | m | [26] 20.11 | i | i |
| 5B | Content-Encoding | [26] 20.12 | m | m | [26] 20.12 | i | i |
| 5C | Content-Language | [26] 20.13 | m | m | [26] 20.13 | i | i |
| 6 | Content-Length | [26] 20.14 | m | m | [26] 20.14 | m | m |
| 7 | Content-Type | [26] 20.15 | m | m | [26] 20.15 | i | i |
| 8 | Cseq | [26] 20.16 | m | m | [26] 20.16 | m | m |
| 9 | Date | [26] 20.17 | m | m | [26] 20.17 | c2 | c2 |
| 10 | Expires | [26] 20.19 | m | m | [26] 20.19 | i | i |
| 11 | From | [26] 20.20 | m | m | [26] 20.20 | m | m |
| 12 | Max-Forwards | [26] 20.22 | m | m | [26] 20.22 | m | m |
| 13 | MIME-Version | [26] 20.24 | m | m | [26] 20.24 | i | i |
| 14 | Organization | [26] 20.25 | m | m | [26] 20.25 | c3 | c3 |
| 14A | P-Access-Network-Info | [52] 4.4 | c22 | c22 | [52] 4.4 | c23 | c23 |
| 14B | P-Asserted-Identity | [34] 9.1 | c9 | c9 | [34] 9.1 | c10 | c10 |
| 14C | P-Called-Party-ID | [52] 4.2 | c13 | c13 | [52] 4.2 | c14 | c15 |
| 14D | P-Charging-Function-Addresses | [52] 4.5 | c20 | c20 | [52] 4.5 | c21 | c21 |
| 14E | P-Charging-Vector | [52] 4.6 | c18 | c18 | [52] 4.6 | c19 | c19 |
| 14F | P-Preferred-Identity | [34] 9.2 | x | x | [34] 9.2 | c8 | c8 |
| 14G | P-Visited-Network-ID | [52] 4.3 | c16 | n/a | [52] 4.3 | c17 | n/a |
| 14H | Privacy | [33] 4.2 | c11 | c11 | [33] 4.2 | c12 | c12 |
| 15 | Proxy-Authorization | [26] 20.28 | m | m | [26] 20.28 | c4 | c4 |
| 16 | Proxy-Require | [26] 20.29 | m | m | [26] 20.29 | m | m |
| 16A | Reason | [34A] 2 | c25 | c25 | [34A] 2 | c26 | c26 |
| 17 | Record-Route | [26] 20.30 | m | m | [26] 20.30 | c7 | c7 |
| 18 | Refer-To | [36] 3 | c3 | c3 | [36] 3 | c4 | c4 |
| 18A | Referred-By | [59] 3 | c29 | c29 | [59] 3 | c30 | c30 |
| 18B | Reject-Contact | [56B] 9.2 | c27 | c27 | [56B] 9.2 | c27 | c28 |
| 18C | Request-Disposition | [56B] 9.1 | c27 | c27 | [56B] 9.1 | c27 | c27 |
| 19 | Require | [26] 20.32 | m | m | [26] 20.32 | c5 | c5 |
| 20 | Route | [26] 20.34 | m | m | [26] 20.34 | m | m |
| 20A | Security-Client | [48] 2.3.1 | x | x | [48] 2.3.1 | c24 | c24 |
| 20B | Security-Verify | [48] 2.3.1 | x | x | [48] 2.3.1 | c24 | c24 |
| 21 | Supported | [26] 20.37 | m | m | [26] 20.37 | c6 | c6 |
| 22 | Timestamp | [26] 20.38 | m | m | [26] 20.38 | i | i |
| 23 | To | [26] 20.39 | m | m | [26] 20.39 | m | m |
| 24 | User-Agent | [26] 20.41 | m | m | [26] 20.41 | i | i |
| 25 | Via | [26] 20.42 | m | m | [26] 20.42 | m | m |

| | |
|---|---|
| c1: | IF A.4/20 THEN m ELSE i - - SIP specific event notification extension. |
| c2: | IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses. |
| c3: | IF A.162/19A OR A.162/19B THEN m ELSE i - - reading, adding or concatenating the Organization header. |
| c4: | IF A.162/8A THEN m ELSE i - - authentication between UA and proxy. |
| c5: | IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER. |
| c6: | IF A.162/16 THEN m ELSE i - - reading the contents of the Supported header before proxying the response. |
| c7: | IF A.162/14 THEN m ELSE i - - the requirement to be able to insert itself in the subsequent transactions in a dialog. |
| c8: | IF A.162/30A THEN m ELSE n/a - - act as first entity within the trust domain for asserted identity. |
| c9: | IF A.162/30 THEN m ELSE n/a - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks. |
| c10: | IF A.162/30A or A.162/30B THEN m ELSE i - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks or subsequent entity within trust network that can route outside the trust network. |
| c11: | IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP). |
| c12: | IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently. |
| c13: | IF A.162/37 THEN m ELSE n/a - - the P-Called-Party-ID header extension. |
| c14: | IF A.162/37 THEN i ELSE n/a - - the P-Called-Party-ID header extension. |
| c15: | IF A.162/37 AND A.3/2 THEN m ELSE IF A.162/37 AND A.3/3 THEN i ELSE n/a - - the P-Called-Party-ID header extension and P-CSCF or I-CSCF. |
| c16: | IF A.162/38 THEN m ELSE n/a - - the P-Visited-Network-ID header extension. |
| c17: | IF A.162/39 THEN m ELSE i - - reading, or deleting the P-Visited-Network-ID header before proxying the request or response. |
| c18: | IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension. |
| c19: | IF A.162/46 THEN m ELSE IF A.162/45 THEN i ELSE n/a - - adding, deleting, reading or modifying the P-Charging-Vector header before proxying the request or response or the P-Charging-Vector header extension. |
| c20: | IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension. |
| c21: | IF A.162/44A THEN m ELSE IF A.162/44 THEN i ELSE n/a - - adding, deleting or reading the P-Charging-Function-Addresses header before proxying the request or response, or the P-Charging-Function-Addresses header extension. |
| c22: | IF A.162/43 THEN x ELSE IF A.162/41 THEN m ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension. |
| c23: | IF A.162/43 THEN m ELSE IF A.162/41 THEN i ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension. |
| c24: | IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. |
| c25: | IF A.162/48 THEN m ELSE n/a - - the Reason header field for the session initiation protocol. |
| c26: | IF A.162/48 THEN i ELSE n/a - - the Reason header field for the session initiation protocol. |
| c27: | IF A.162/50 THEN m ELSE n/a - - caller preferences for the session initiation protocol. |
| c28: | IF A.162/50 AND A.4/3 THEN m ELSE IF A.162/50 AND NOT A.4/3 THEN i ELSE n/a - - caller preferences for the session initiation protocol, and S-CSCF. |
| c29: | IF A.162/53 THEN i ELSE n/a - - the SIP Referred-By mechanism. |
| c30: | IF A.162/53 THEN m ELSE n/a - - the SIP Referred-By mechanism. |
| NOTE: | c1 refers to the UA role major capability as this is the case of a proxy that also acts as a UA specifically for SUBSCRIBE and NOTIFY. |

Prerequisite A.163/16 - - REFER request

**Table A.262: Supported message bodies within the REFER request**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | | | | | | | |

**Table A.263: Void**

Prerequisite A.163/17 - - REFER response for all status-codes

**Table A.264: Supported headers within the REFER response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 0A | Allow | [26] 20.5 | m | m | [26] 20.5 | i | i |
| 1 | Call-ID | [26] 20.8 | m | m | [26] 20.8 | m | m |
| 1A | Contact | [26] 20.10 | m | m | [26] 20.10 | i | i |
| 1B | Content-Disposition | [26] 20.11 | m | m | [26] 20.11 | i | i |
| 2 | Content-Encoding | [26] 20.12 | m | m | [26] 20.12 | i | i |
| 3 | Content-Language | [26] 20.13 | m | m | [26] 20.13 | i | i |
| 4 | Content-Length | [26] 20.14 | m | m | [26] 20.14 | m | m |
| 5 | Content-Type | [26] 20.15 | m | m | [26] 20.15 | i | i |
| 6 | Cseq | [26] 20.16 | m | m | [26] 20.16 | m | m |
| 7 | Date | [26] 20.17 | m | m | [26] 20.17 | c1 | c1 |
| 8 | From | [26] 20.20 | m | m | [26] 20.20 | m | m |
| 9 | MIME-Version | [26] 20.24 | m | m | [26] 20.24 | i | i |
| 10 | Organization | [26] 20.25 | m | m | [26] 20.25 | c2 | c2 |
| 10A | P-Access-Network-Info | [52] 4.4 | c12 | c12 | [52] 4.4 | c13 | c13 |
| 10B | P-Asserted-Identity | [34] 9.1 | c4 | c4 | [34] 9.1 | c5 | c5 |
| 10C | P-Charging-Function-Addresses | [52] 4.5 | c10 | c10 | [52] 4.5 | c11 | c11 |
| 10D | P-Charging-Vector | [52] 4.6 | c8 | c8 | [52] 4.6 | c9 | c9 |
| 10E | P-Preferred-Identity | [34] 9.2 | x | x | [34] 9.2 | c3 | n/a |
| 10F | Privacy | [33] 4.2 | c6 | c6 | [33] 4.2 | c7 | c7 |
| 10G | Require | [26] 20.32 | m | m | [26] 20.32 | c14 | c14 |
| 10H | Server | [26] 20.35 | m | m | [26] 20.35 | i | i |
| 11 | Timestamp | [26] 20.38 | m | m | [26] 20.38 | i | i |
| 12 | To | [26] 20.39 | m | m | [26] 20.39 | m | m |
| 12A | User-Agent | [26] 20.41 | m | m | [26] 20.41 | i | i |
| 13 | Via | [26] 20.42 | m | m | [26] 20.42 | m | m |
| 14 | Warning | [26] 20.43 | m | m | [26] 20.43 | i | i |

c1: IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses.
c2: IF A.162/19A OR A.162/19B THEN m ELSE i - - reading, adding or concatenating the Organization header.
c3: IF A.162/30A THEN m ELSE n/a - - act as first entity within the trust domain for asserted identity.
c4: IF A.162/30 THEN m ELSE n/a - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.
c5: IF A.162/30A or A.162/30B THEN m ELSE i - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks or subsequent entity within trust network that can route outside the trust network.
c6: IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c7: IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently.
c8: IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.
c9: IF A.162/46 THEN m ELSE IF A.162/45 THEN i ELSE n/a - - adding, deleting, reading or modifying the P-Charging-Vector header before proxying the request or response or the P-Charging-Vector header extension.
c10: IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.
c11: IF A.162/44A THEN m ELSE IF A.162/44 THEN i ELSE n/a - - adding, deleting or reading the P-Charging-Function-Addresses header before proxying the request or response, or the P-Charging-Function-Addresses header extension.
c12: IF A.162/43 THEN x ELSE IF A.162/41 THEN m ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.
c13: IF A.162/43 THEN m ELSE IF A.162/41 THEN i ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.
c14: IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER.

Prerequisite A.163/17 - - REFER response

Prerequisite: A.164/102 - - Additional for 2xx response

**Table A.265: Supported headers within the REFER response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Allow-Events | [28] 7.2.2 | m | m | [28] 7.2.2 | c1 | c1 |
| 2 | Authentication-Info | [26] 20.6 | m | m | [26] 20.6 | i | i |
| 5 | Record-Route | [26] 20.30 | m | m | [26] 20.30 | c3 | c3 |
| 8 | Supported | [26] 20.37 | m | m | [26] 20.37 | i | i |
| c1: IF A.4/20 THEN m ELSE i - - SIP specific event notification extension.<br>c3: IF A.162/15 THEN m ELSE i - - the requirement to be able to use separate URIs in the upstream direction and downstream direction when record routeing. | | | | | | | |

Prerequisite A.163/17 - - REFER response

Prerequisite: A.164/103 OR A.164/104 OR A.164/105 OR A.164/106 - - Additional for 3xx – 6xx response

**Table A.265A: Supported headers within the REFER response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Error-Info | [26] 20.18 | m | m | [26] 20.18 | i | i |

**Table A.266: Void**

Prerequisite A.163/17 - - REFER response

Prerequisite: A.164/8 OR A.164/9 OR A.164/10 OR A.164/11 OR A.164/12 - - Additional for 401 (Unauthorized) response

**Table A.267: Supported headers within the REFER response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 4 | Proxy-Authenticate | [26] 20.27 | m | m | [26] 20.27 | m | m |
| 10 | WWW-Authenticate | [26] 20.44 | m | m | [26] 20.44 | i | i |

Prerequisite A.163/17 - - REFER response

Prerequisite: A.164/17 OR A.164/23 OR A.164/30 OR A.164/36 OR A.164/42 OR A.164/45 OR A.164/50 OR A.164/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response

**Table A.268: Supported headers within the REFER response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 6 | Retry-After | [26] 20.33 | m | m | [26] 20.33 | i | i |

**Table A.269: Void**

Prerequisite A.163/17 - - REFER response

Prerequisite: A.164/20 - - Additional for 407 (Proxy Authentication Required) response

**Table A.270: Supported headers within the REFER response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 4 | Proxy-Authenticate | [26] 20.27 | o | | [26] 20.27 | o | |
| 8 | WWW-Authenticate | [26] 20.44 | m | m | [26] 20.44 | i | i |

Prerequisite A.163/17 - - REFER response

Prerequisite: A.164/25 - - Additional for 415 (Unsupported Media Type) response

**Table A.271: Supported headers within the REFER response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Accept | [26] 20.1 | m | m | [26] 20.1 | i | i |
| 2 | Accept-Encoding | [26] 20.2 | m | m | [26] 20.2 | i | i |
| 3 | Accept-Language | [26] 20.3 | m | m | [26] 20.3 | i | i |

Prerequisite A.163/17 - - REFER response

Prerequisite: A.164/27 - - Additional for 420 (Bad Extension) response

**Table A.272: Supported headers within the REFER response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 8 | Unsupported | [26] 20.40 | m | m | [26] 20.40 | c3 | c3 |
| c3: | IF A.162/18 THEN m ELSE i - - reading the contents of the Unsupported header before proxying the 420 response to a method other than REGISTER. | | | | | | |

Prerequisite A.163/17 - - REFER response

Prerequisite: A.164/28 OR A.164/41A - - Additional for 421 (Extension Required), 494 (Security Agreement Required) response

**Table A.272A: Supported headers within the REFER response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 3 | Security-Server | [48] 2 | c1 | c1 | [48] 2 | n/a | n/a |
| c1: | IF A.162/47 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. | | | | | | |

**Table A.273: Void**

Prerequisite A.163/17 - - REFER response

**Table A.274: Supported message bodies within the REFER response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | | | | | | | |

### A.2.2.4.12 REGISTER method

Prerequisite A.163/18 - - REGISTER request

**Table A.275: Supported headers within the REGISTER request**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Accept | [26] 20.1 | m | m | [26] 20.1 | i | i |
| 2 | Accept-Encoding | [26] 20.2 | m | m | [26] 20.2 | i | i |
| 3 | Accept-Language | [26] 20.3 | m | m | [26] 20.3 | i | i |
| 3A | Allow | [26] 20.5 | m | m | [26] 20.5 | i | i |
| 4 | Allow-Events | [28] 7.2.2 | m | m | [28] 7.2.2 | c1 | c1 |
| 5 | Authorization | [26] 20.7, [49] | m | m | [26] 20.7, [49] | i | i |
| 6 | Call-ID | [26] 20.8 | m | m | [26] 20.8 | m | m |
| 7 | Call-Info | [26] 20.9 | m | m | [26] 20.9 | c2 | c2 |
| 8 | Contact | [26] 20.10 | m | m | [26] 20.10 | i | i |
| 9 | Content-Disposition | [26] 20.11 | m | m | [26] 20.11 | i | i |
| 10 | Content-Encoding | [26] 20.12 | m | m | [26] 20.12 | i | i |
| 11 | Content-Language | [26] 20.13 | m | m | [26] 20.13 | i | i |
| 12 | Content-Length | [26] 20.14 | m | m | [26] 20.14 | m | m |
| 13 | Content-Type | [26] 20.15 | m | m | [26] 20.15 | i | i |
| 14 | Cseq | [26] 20.16 | m | m | [26] 20.16 | m | m |
| 15 | Date | [26] 20.17 | m | m | [26] 20.17 | m | m |
| 16 | Expires | [26] 20.19 | m | m | [26] 20.19 | i | i |
| 17 | From | [26] 20.20 | m | m | [26] 20.20 | m | m |
| 18 | Max-Forwards | [26] 20.22 | m | m | [26] 20.22 | m | m |
| 19 | MIME-Version | [26] 20.24 | m | m | [26] 20.24 | i | i |
| 20 | Organization | [26] 20.25 | m | m | [26] 20.25 | c3 | c3 |
| 20A | P-Access-Network-Info | [52] 4.4 | c16 | c16 | [52] 4.4 | c17 | c17 |
| 20B | P-Charging-Function-Addresses | [52] 4.5 | c14 | c14 | [52] 4.5 | c15 | c15 |
| 20C | P-Charging-Vector | [52] 4.6 | c12 | c12 | [52] 4.6 | c13 | c13 |
| 20D | P-Visited-Network-ID | [52] 4.3 | c10 | c10 | [52] 4.3 | c11 | c11 |
| 20E | Path | [35] 4.2 | c6 | c6 | [35] 4.2 | c6 | c6 |
| 20F | Privacy | [33] 4.2 | c8 | c8 | [33] 4.2 | c9 | c9 |
| 21 | Proxy-Authorization | [26] 20.28 | m | m | [26] 20.28 | c7 | c7 |
| 22 | Proxy-Require | [26] 20.29 | m | m | [26] 20.29 | m | m |
| 22A | Reason | [34A] 2 | c19 | c19 | [34A] 2 | c20 | c20 |
| 22B | Referred-By | [59] 3 | c22 | c22 | [59] 3 | c23 | c23 |
| 22C | Request-Disposition | [56B] 9.1 | c21 | c21 | [56B] 9.1 | c21 | c21 |
| 23 | Require | [26] 20.32 | m | m | [26] 20.32 | c4 | c4 |
| 24 | Route | [26] 20.34 | m | m | [26] 20.34 | m | m |
| 24A | Security-Client | [48] 2.3.1 | x | x | [48] 2.3.1 | c18 | c18 |
| 24B | Security-Verify | [48] 2.3.1 | x | x | [48] 2.3.1 | c18 | c18 |
| 25 | Supported | [26] 20.37 | m | m | [26] 20.37 | c5 | c5 |
| 26 | Timestamp | [26] 20.38 | m | m | [26] 20.38 | i | i |
| 27 | To | [26] 20.39 | m | m | [26] 20.39 | m | m |
| 28 | User-Agent | [26] 20.41 | m | m | [26] 20.41 | i | i |
| 29 | Via | [26] 20.42 | m | m | [26] 20.42 | m | m |

| | |
|---|---|
| c1: | IF A.4/20 THEN m ELSE i - - SIP specific event notification extension. |
| c2: | IF A.162/19C OR A.162/19D THEN m ELSE i - - reading, adding or concatenating the Call-Info header. |
| c3: | IF A.162/19A OR A.162/19B THEN m ELSE i - - reading, adding or concatenating the Organization header. |
| c4: | IF A.162/11 OR A.162/12 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER. |
| c5: | IF A.162/16 THEN m ELSE i - - reading the contents of the Supported header before proxying the response. |
| c6: | IF A.162/29 THEN m ELSE n/a - - PATH header support. |
| c7: | IF A.162/8A THEN m ELSE i - - authentication between UA and proxy. |
| c8: | IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP). |
| c9: | IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently. |
| c10: | IF A.162/38 THEN m ELSE n/a - - the P-Visited-Network-ID header extension. |
| c11: | IF A.162/39 THEN m ELSE i - - reading, or deleting the P-Visited-Network-ID header before proxying the request or response. |
| c12: | IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension. |
| c13: | IF A.162/46 THEN m ELSE IF A.162/45 THEN i ELSE n/a - - adding, deleting, reading or modifying the P-Charging-Vector header before proxying the request or response or the P-Charging-Vector header extension. |
| c14: | IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension. |
| c15: | IF A.162/44A THEN m ELSE IF A.162/44 THEN i ELSE n/a - - adding, deleting or reading the P-Charging-Function-Addresses header before proxying the request or response, or the P-Charging-Function-Addresses header extension. |
| c16: | IF A.162/43 THEN x ELSE IF A.162/41 THEN m ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension. |
| c17: | IF A.162/43 THEN m ELSE IF A.162/41 THEN i ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension. |
| c18: | IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. |
| c19: | IF A.162/48 THEN m ELSE n/a - - the Reason header field for the session initiation protocol. |
| c20: | IF A.162/48 THEN i ELSE n/a - - the Reason header field for the session initiation protocol. |
| c21: | IF A.162/50 THEN m ELSE n/a - - caller preferences for the session initiation protocol. |
| c22: | IF A.162/53 THEN i ELSE n/a - - the SIP Referred-By mechanism. |
| c23: | IF A.162/53 THEN m ELSE n/a - - the SIP Referred-By mechanism. |
| NOTE: | c1 refers to the UA role major capability as this is the case of a proxy that also acts as a UA specifically for SUBSCRIBE and NOTIFY. |

Prerequisite A.163/18 - - REGISTER request

**Table A.276: Supported message bodies within the REGISTER request**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | | | | | | | |

**Table A.277: Void**

Prerequisite A.163/19 - - REGISTER response for all status-codes

**Table A.278: Supported headers within the REGISTER response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 0A | Allow | [26] 20.5 | m | m | [26] 20.5 | i | i |
| 1 | Call-ID | [26] 20.8 | m | m | [26] 20.8 | m | m |
| 1A | Call-Info | [26] 20.9 | m | m | [26] 20.9 | c2 | c2 |
| 2 | Content-Disposition | [26] 20.11 | m | m | [26] 20.11 | i | i |
| 3 | Content-Encoding | [26] 20.12 | m | m | [26] 20.12 | i | i |
| 4 | Content-Language | [26] 20.13 | m | m | [26] 20.13 | i | i |
| 5 | Content-Length | [26] 20.14 | m | m | [26] 20.14 | m | m |
| 6 | Content-Type | [26] 20.15 | m | m | [26] 20.15 | i | i |
| 7 | Cseq | [26] 20.16 | m | m | [26] 20.16 | m | m |
| 8 | Date | [26] 20.17 | m | m | [26] 20.17 | m | m |
| 9 | From | [26] 20.20 | m | m | [26] 20.20 | m | m |
| 10 | MIME-Version | [26] 20.24 | m | m | [26] 20.24 | i | i |
| 11 | Organization | [26] 20.25 | m | m | [26] 20.25 | c1 | c1 |
| 11A | P-Access-Network-Info | [52] 4.4 | c9 | c9 | [52] 4.4 | c10 | c10 |
| 11B | P-Charging-Function-Addresses | [52] 4.5 | c7 | c7 | [52] 4.5 | c8 | c8 |
| 11C | P-Charging-Vector | [52] 4.6 | c5 | c5 | [52] 4.6 | c6 | c6 |
| 11D | Privacy | [33] 4.2 | c3 | c3 | [33] 4.2 | c4 | c4 |
| 11E | Require | [26] 20.32 | m | m | [26] 20.32 | c11 | c11 |
| 11F | Server | [26] 20.35 | m | m | [26] 20.35 | i | i |
| 12 | Timestamp | [26] 20.38 | m | m | [26] 20.38 | i | i |
| 13 | To | [26] 20.39 | m | m | [26] 20.39 | m | m |
| 13A | User-Agent | [26] 20.41 | m | m | [26] 20.41 | i | i |
| 14 | Via | [26] 20.42 | m | m | [26] 20.42 | m | m |
| 15 | Warning | [26] 20.43 | m | m | [26] 20.43 | i | i |

c1: IF A.162/19A OR A.162/19B THEN m ELSE i - - reading, adding or concatenating the Organization header.
c2: IF A.162/19C OR A.162/19D THEN m ELSE i - - reading, adding or concatenating the Call-Info header.
c3: IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c4: IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently.
c5: IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.
c6: IF A.162/46 THEN m ELSE IF A.162/45 THEN i ELSE n/a - - adding, deleting, reading or modifying the P-Charging-Vector header before proxying the request or response or the P-Charging-Vector header extension.
c7: IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.
c8: IF A.162/44A THEN m ELSE IF A.162/44 THEN i ELSE n/a - - adding, deleting or reading the P-Charging-Function-Addresses header before proxying the request or response, or the P-Charging-Function-Addresses header extension.
c9: IF A.162/43 THEN x ELSE IF A.162/41 THEN m ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.
c10: IF A.162/43 THEN m ELSE IF A.162/41 THEN i ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.
c11: IF A.162/11 OR A.162/12 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER.

Prerequisite A.163/19 - - REGISTER response

Prerequisite: A.164/102 - - Additional for 2xx response

**Table A.279: Supported headers within the REGISTER response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Accept | [26] 20.1 | m | m | [26] 20.1 | i | i |
| 1A | Accept-Encoding | [26] 20.2 | m | m | [26] 20.2 | i | i |
| 1B | Accept-Language | [26] 20.3 | m | m | [26] 20.3 | i | i |
| 2 | Allow-Events | [28] 7.2.2 | m | m | [28] 7.2.2 | c1 | c1 |
| 3 | Authentication-Info | [26] 20.6 | m | m | [26] 20.6 | i | i |
| 5 | Contact | [26] 20.10 | m | m | [26] 20.10 | i | i |
| 5A | P-Associated-URI | [52] 4.1 | c8 | c8 | [52] 4.1 | c9 | c10 |
| 6 | Path | [35] 4.2 | c3 | c3 | [35] 4.2 | c4 | c4 |
| 8 | Service-Route | [38] 5 | c5 | c5 | [38] 5 | c6 | c7 |
| 9 | Supported | [26] 20.37 | m | m | [26] 20.37 | i | i |
| c1: | IF A.4/20 THEN m ELSE i - - SIP specific event notification extension. | | | | | | |
| c2: | IF A.3/2 OR A.3/3A THEN m ELSE n/a - - P-CSCF or I-CSCF (THIG). | | | | | | |
| c3: | IF A.162/29 THEN m ELSE n/a - - Path extension support. | | | | | | |
| c4: | IF A.162/29 THEN i ELSE n/a - - Path extension support. | | | | | | |
| c5: | IF A.162/32 THEN m ELSE n/a - - Service-Route extension support. | | | | | | |
| c6: | IF A.162/32 THEN i ELSE n/a - - Service-Route extension support. | | | | | | |
| c7: | IF A.162/32 THEN (IF A.3/2 THEN m ELSE i) ELSE n/a - - Service-Route extension and P-CSCF. | | | | | | |
| c8: | IF A.162/36 THEN m ELSE n/a - - the P-Associated-URI extension. | | | | | | |
| c9: | IF A.162/36 THEN i ELSE n/a - - the P-Associated-URI extension. | | | | | | |
| c10: | IF A.162/36 AND A.3/2 THEN m ELSE IF A.162/36 AND A.3/3 THEN i ELSE n/a - - the P-Associated-URI extension and P-CSCF or I-CSCF. | | | | | | |

Prerequisite A.163/19 - - REGISTER response

Prerequisite: A.164/103 OR A.164/104 OR A.164/105 OR A.164/106 - - Additional for 3xx – 6xx response

**Table A.171A: Supported headers within the REGISTER response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Error-Info | [26] 20.18 | m | m | [26] 20.18 | i | i |

Prerequisite A.163/19 - - REGISTER response

Prerequisite: A.164/103 OR A.164/35 - - Additional for 3xx or 485 (Ambiguous) response

**Table A.280: Supported headers within the REGISTER response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 3 | Contact | [26] 20.10 | m | m | [26] 20.10 | c2 | c2 |
| c2: | IF A.162/19E THEN m ELSE i - - deleting Contact headers. | | | | | | |

Prerequisite A.163/19 - - REGISTER response

Prerequisite: A.164/14 - - Additional for 401 (Unauthorized) response

**Table A.281: Supported headers within the REGISTER response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 4 | Proxy-Authenticate | [26] 20.27 | m | m | [26] 20.27 | m | m |
| 6 | Security-Server | [48] 2 | x | c1 | [48] 2 | n/a | n/a |
| 10 | WWW-Authenticate | [26] 20.44 | m | m | [26] 20.44 | i | i |
| c1: | IF A.162/47 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. | | | | | | |

Prerequisite A.163/19 - - REGISTER response

Prerequisite: A.164/17 OR A.164/23 OR A.164/30 OR A.164/36 OR A.164/42 OR A.164/45 OR A.164/50 OR A.164/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response

**Table A.282: Supported headers within the REGISTER response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 6 | Retry-After | [26] 20.33 | m | m | [26] 20.33 | i | i |

**Table A.283: Void**

Prerequisite A.163/19 - - REGISTER response

Prerequisite: A.164/20 - - Additional for 407 (Proxy Authentication Required) response

**Table A.284: Supported headers within the REGISTER response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 5 | Proxy-Authenticate | [26] 20.27 | m | m | [26] 20.27 | m | m |
| 9 | WWW-Authenticate | [26] 20.44 | m | m | [26] 20.44 | i | i |

Prerequisite A.163/19 - - REGISTER response

Prerequisite: A.164/25 - - Additional for 415 (Unsupported Media Type) response

**Table A.285: Supported headers within the REGISTER response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Accept | [26] 20.1 | m | m | [26] 20.1 | i | i |
| 2 | Accept-Encoding | [26] 20.2 | m | m | [26] 20.2 | i | i |
| 3 | Accept-Language | [26] 20.3 | m | m | [26] 20.3 | i | i |

Prerequisite A.163/19 - - REGISTER response

Prerequisite: A.164/27 - - Additional for 420 (Bad Extension) response

**Table A.286: Supported headers within the REGISTER response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 8 | Unsupported | [26] 20.40 | m | m | [26] 20.40 | c3 | c3 |
| c3: | IF A.162/17 THEN m ELSE.i | | | | | | |

Prerequisite A.163/19 - - REGISTER response

Prerequisite: A.164/28 OR A.164/41A - - Additional for 421 (Extension Required), 494 (Security Agreement Required) response

**Table A.286A: Supported headers within the REGISTER response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 3 | Security-Server | [48] 2 | c1 | c1 | [48] 2 | n/a | n/a |
| c1: | IF A.162/47 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. | | | | | | |

Prerequisite A.163/19 - - REGISTER response

Prerequisite: A.164/29 - - Additional for 423 (Interval Too Brief) response

**Table A.287: Supported headers within the REGISTER response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 5 | Min-Expires | [26] 20.23 | m | m | [26] 20.23 | i | i |

**Table A.288: Void**

Prerequisite A.163/19 - - REGISTER response

**Table A.289: Supported message bodies within the REGISTER response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | | | | | | | |

### A.2.2.4.13 SUBSCRIBE method

Prerequisite A.163/20 - - SUBSCRIBE request

**Table A.290: Supported headers within the SUBSCRIBE request**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Accept | [26] 20.1 | m | m | [26] 20.1 | i | i |
| 1A | Accept-Contact | [56B] 9.2 | c27 | c27 | [56B] 9.2 | c27 | c28 |
| 2 | Accept-Encoding | [26] 20.2 | m | m | [26] 20.2 | i | i |
| 3 | Accept-Language | [26] 20.3 | m | m | [26] 20.3 | i | i |
| 3A | Allow | [26] 20.5 | m | m | [26] 20.5 | i | i |
| 4 | Allow-Events | [28] 7.2.2 | m | m | [28] 7.2.2 | c1 | c1 |
| 5 | Authorization | [26] 20.7 | m | m | [26] 20.7 | i | i |
| 6 | Call-ID | [26] 20.8 | m | m | [26] 20.8 | m | m |
| 6A | Contact | [26] 20.10 | m | m | [26] 20.10 | i | i |
| 7 | Content-Disposition | [26] 20.11 | m | m | [26] 20.11 | i | i |
| 8 | Content-Encoding | [26] 20.12 | m | m | [26] 20.12 | i | i |
| 9 | Content-Language | [26] 20.13 | m | m | [26] 20.13 | i | i |
| 10 | Content-Length | [26] 20.14 | m | m | [26] 20.14 | m | m |
| 11 | Content-Type | [26] 20.15 | m | m | [26] 20.15 | i | i |
| 12 | Cseq | [26] 20.16 | m | m | [26] 20.16 | m | m |
| 13 | Date | [26] 20.17 | m | m | [26] 20.17 | c2 | c2 |
| 14 | Event | [28] 7.2.1 | m | m | [28] 7.2.1 | m | m |
| 15 | Expires | [26] 20.19 | m | m | [26] 20.19 | i | i |
| 16 | From | [26] 20.20 | m | m | [26] 20.20 | m | m |
| 17 | Max-Forwards | [26] 20.22 | m | m | [26] 20.22 | m | m |
| 18 | MIME-Version | [26] 20.24 | m | m | [26] 20.24 | i | i |
| 18A | Organization | [26] 20.25 | m | m | [26] 20.25 | c3 | c3 |
| 18B | P-Access-Network-Info | [52] 4.4 | c22 | c22 | [52] 4.4 | c23 | c23 |
| 18C | P-Asserted-Identity | [34] 9.1 | c9 | c9 | [34] 9.1 | c10 | c10 |
| 18D | P-Called-Party-ID | [52] 4.2 | c13 | c13 | [52] 4.2 | c14 | c15 |
| 18E | P-Charging-Function-Addresses | [52] 4.5 | c20 | c20 | [52] 4.5 | c21 | c21 |
| 18F | P-Charging-Vector | [52] 4.6 | c18 | c18 | [52] 4.6 | c19 | c19 |
| 18G | P-Preferred-Identity | [34] 9.2 | x | x | [34] 9.2 | c8 | c8 |
| 18H | P-Visited-Network-ID | [52] 4.3 | c16 | n/a | [52] 4.3 | c17 | n/a |
| 18I | Privacy | [33] 4.2 | c11 | c11 | [33] 4.2 | c12 | c12 |
| 19 | Proxy-Authorization | [26] 20.28 | m | m | [26] 20.28 | c4 | c4 |
| 20 | Proxy-Require | [26] 20.29 | m | m | [26] 20.29 | m | m |
| 20A | Reason | [34A] 2 | c25 | c25 | [34A] 2 | c26 | c26 |
| 21 | Record-Route | [26] 20.30 | m | m | [26] 20.30 | c7 | c7 |
| 21A | Referred-By | [59] 3 | c29 | c29 | [59] 3 | c30 | c30 |
| 21B | Reject-Contact | [56B] 9.2 | c27 | c27 | [56B] 9.2 | c27 | c28 |
| 21C | Request-Disposition | [56B] 9.1 | c27 | c27 | [56B] 9.1 | c27 | c27 |
| 22 | Require | [26] 20.32 | m | m | [26] 20.32 | c5 | c5 |
| 23 | Route | [26] 20.34 | m | m | [26] 20.34 | m | m |
| 23A | Security-Client | [48] 2.3.1 | x | x | [48] 2.3.1 | c24 | c24 |
| 23B | Security-Verify | [48] 2.3.1 | x | x | [48] 2.3.1 | c24 | c24 |
| 24 | Supported | [26] 20.37 | m | m | [26] 20.37 | c6 | c6 |
| 25 | Timestamp | [26] 20.38 | m | m | [26] 20.38 | i | i |
| 26 | To | [26] 20.39 | m | m | [26] 20.39 | m | m |
| 27 | User-Agent | [26] 20.41 | m | m | [26] 20.41 | i | i |
| 28 | Via | [26] 20.42 | m | m | [26] 20.42 | m | m |

| | |
|---|---|
| c1: | IF A.4/20 THEN m ELSE i - - SIP specific event notification extension. |
| c2: | IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses. |
| c3: | IF A.162/19A OR A.162/19B THEN m ELSE i - - reading, adding or concatenating the Organization header. |
| c4: | IF A.162/8A THEN m ELSE i - - authentication between UA and proxy. |
| c5: | IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER. |
| c6: | IF A.162/16 THEN m ELSE i - - reading the contents of the Supported header before proxying the response. |
| c7: | IF A.162/14 THEN m ELSE i - - the requirement to be able to insert itself in the subsequent transactions in a dialog. |
| c8: | IF A.162/30A THEN m ELSE n/a - - act as first entity within the trust domain for asserted identity. |
| c9: | IF A.162/30 THEN m ELSE n/a - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks. |
| c10: | IF A.162/30A or A.162/30B THEN m ELSE i - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks or subsequent entity within trust network that can route outside the trust network. |
| c11: | IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP). |
| c12: | IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently. |
| c13: | IF A.162/37 THEN m ELSE n/a - - the P-Called-Party-ID header extension. |
| c14: | IF A.162/37 THEN i ELSE n/a - - the P-Called-Party-ID header extension. |
| c15: | IF A.162/37 AND A.3/2 THEN m ELSE IF A.162/37 AND A.3/3 THEN i ELSE n/a - - the P-Called-Party-ID header extension and P-CSCF or I-CSCF. |
| c16: | IF A.162/38 THEN m ELSE n/a - - the P-Visited-Network-ID header extension. |
| c17: | IF A.162/39 THEN m ELSE i - - reading, or deleting the P-Visited-Network-ID header before proxying the request or response. |
| c18: | IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension. |
| c19: | IF A.162/46 THEN m ELSE IF A.162/45 THEN i ELSE n/a - - adding, deleting, reading or modifying the P-Charging-Vector header before proxying the request or response or the P-Charging-Vector header extension. |
| c20: | IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension. |
| c21: | IF A.162/44A THEN m ELSE IF A.162/44 THEN i ELSE n/a - - adding, deleting or reading the P-Charging-Function-Addresses header before proxying the request or response, or the P-Charging-Function-Addresses header extension. |
| c22: | IF A.162/43 THEN x ELSE IF A.162/41 THEN m ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension. |
| c23: | IF A.162/43 THEN m ELSE IF A.162/41 THEN i ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension. |
| c24: | IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. |
| c25: | IF A.162/48 THEN m ELSE n/a - - the Reason header field for the session initiation protocol. |
| c26: | IF A.162/48 THEN i ELSE n/a - - the Reason header field for the session initiation protocol. |
| c27: | IF A.162/50 THEN m ELSE n/a - - caller preferences for the session initiation protocol. |
| c28: | IF A.162/50 AND A.4/3 THEN m ELSE IF A.162/50 AND NOT A.4/3 THEN i ELSE n/a - - caller preferences for the session initiation protocol, and S-CSCF. |
| c29: | IF A.162/53 THEN i ELSE n/a - - the SIP Referred-By mechanism. |
| c30: | IF A.162/53 THEN m ELSE n/a - - the SIP Referred-By mechanism. |
| NOTE: | c1 refers to the UA role major capability as this is the case of a proxy that also acts as a UA specifically for SUBSCRIBE and NOTIFY. |

Prerequisite A.163/20 - - SUBSCRIBE request

**Table A.291: Supported message bodies within the SUBSCRIBE request**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | | | | | | | |

Prerequisite A.163/21 - - SUBSCRIBE response for all status-codes

**Table A.292: Supported headers within the SUBSCRIBE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 0A | Allow | [26] 20.5 | m | m | [26] 20.5 | i | i |
| 1 | Call-ID | [26] 20.8 | m | m | [26] 20.8 | m | m |
| 2 | Content-Disposition | [26] 20.11 | m | m | [26] 20.11 | i | i |
| 3 | Content-Encoding | [26] 20.12 | m | m | [26] 20.12 | i | i |
| 4 | Content-Language | [26] 20.13 | m | m | [26] 20.13 | i | i |
| 5 | Content-Length | [26] 20.14 | m | m | [26] 20.14 | m | m |
| 6 | Content-Type | [26] 20.15 | m | m | [26] 20.15 | i | i |
| 7 | Cseq | [26] 20.16 | m | m | [26] 20.16 | m | m |
| 8 | Date | [26] 20.17 | m | m | [26] 20.17 | c1 | c1 |
| 9 | From | [26] 20.20 | m | m | [26] 20.20 | m | m |
| 10 | MIME-Version | [26] 20.24 | m | m | [26] 20.24 | i | i |
| 10A | Organization | [26] 20.25 | m | m | [26] 20.25 | c2 | c2 |
| 10B | P-Access-Network-Info | [52] 4.4 | c12 | c12 | [52] 4.4 | c13 | c13 |
| 10C | P-Asserted-Identity | [34] 9.1 | c4 | c4 | [34] 9.1 | c5 | c5 |
| 10D | P-Charging-Function-Addresses | [52] 4.5 | c10 | c10 | [52] 4.5 | c11 | c11 |
| 10E | P-Charging-Vector | [52] 4.6 | c8 | c8 | [52] 4.6 | c9 | c9 |
| 10F | P-Preferred-Identity | [34] 9.2 | x | x | [34] 9.2 | c3 | n/a |
| 10G | Privacy | [33] 4.2 | c6 | c6 | [33] 4.2 | c7 | c7 |
| 10H | Require | [26] 20.32 | m | m | [26] 20.32 | c14 | c14 |
| 10I | Server | [26] 20.35 | m | m | [26] 20.35 | i | i |
| 11 | Timestamp | [26] 20.38 | m | m | [26] 20.38 | i | i |
| 12 | To | [26] 20.39 | m | m | [26] 20.39 | m | m |
| 12A | User-Agent | [26] 20.41 | m | m | [26] 20.41 | i | i |
| 13 | Via | [26] 20.42 | m | m | [26] 20.42 | m | m |
| 14 | Warning | [26] 20.43 | m | m | [26] 20.43 | i | i |

c1: IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses.
c2: IF A.162/19A OR A.162/19B THEN m ELSE i - - reading, adding or concatenating the Organization header.
c3: IF A.162/30A THEN m ELSE n/a - - act as first entity within the trust domain for asserted identity.
c4: IF A.162/30 THEN m ELSE n/a - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.
c5: IF A.162/30A or A.162/30B THEN m ELSE i - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks or subsequent entity within trust network that can route outside the trust network.
c6: IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c7: IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently.
c8: IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.
c9: IF A.162/46 THEN m ELSE IF A.162/45 THEN i ELSE n/a - - adding, deleting, reading or modifying the P-Charging-Vector header before proxying the request or response or the P-Charging-Vector header extension.
c10: IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.
c11: IF A.162/44A THEN m ELSE IF A.162/44 THEN i ELSE n/a - - adding, deleting or reading the P-Charging-Function-Addresses header before proxying the request or response, or the P-Charging-Function-Addresses header extension.
c12: IF A.162/43 THEN x ELSE IF A.162/41 THEN m ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.
c13: IF A.162/43 THEN m ELSE IF A.162/41 THEN i ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.
c14: IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER.

Prerequisite A.163/21 - - SUBSCRIBE response

Prerequisite: A.164/102 - - Additional for 2xx response

**Table A.293: Supported headers within the SUBSCRIBE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 0A | Allow-Events | [28] 7.2.2 | m | m | [28] 7.2.2 | i | i |
| 1 | Authentication-Info | [26] 20.6 | m | m | [26] 20.6 | i | i |
| 1A | Contact | [26] 20.10 | m | m | [26] 20.10 | i | i |
| 2 | Expires | [26] 20.19 | m | m | [26] 20.19 | i | i |
| 3 | Record-Route | [26] 20.30 | m | m | [26] 20.30 | c3 | c3 |
| 6 | Supported | [26] 20.37 | m | m | [26] 20.37 | i | i |
| c3: | IF A.162/15 THEN m ELSE i - - the requirement to be able to use separate URIs in the upstream direction and downstream direction when record routeing. | | | | | | |

Prerequisite A.163/21 - - SUBSCRIBE response

Prerequisite: A.164/103 OR A.164/104 OR A.164/105 OR A.164/106 - - Additional for 3xx – 6xx response

**Table A.293A: Supported headers within the SUBSCRIBE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Error-Info | [26] 20.18 | m | m | [26] 20.18 | i | i |

Prerequisite A.163/21 - - SUBSCRIBE response

Prerequisite: A.164/103 OR A.164/35 - - Additional for 3xx or 485 (Ambiguous) response

**Table A.294: Supported headers within the SUBSCRIBE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Contact | [26] 20.10 | m | m | [26] 20.10 | c1 | c1 |
| c1: | IF A.162/19E THEN m ELSE i - - deleting Contact headers. | | | | | | |

Prerequisite A.163/21 - - SUBSCRIBE response

Prerequisite: A.164/14 - - Additional for 401 (Unauthorized) response

**Table A.295: Supported headers within the SUBSCRIBE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 2 | Proxy-Authenticate | [26] 20.27 | m | m | [26] 20.27 | m | m |
| 8 | WWW-Authenticate | [26] 20.44 | m | m | [26] 20.44 | i | i |

Prerequisite A.163/21 - - SUBSCRIBE response

Prerequisite: A.164/17 OR A.164/23 OR A.164/30 OR A.164/36 OR A.164/42 OR A.164/45 OR A.164/50 OR A.164/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480 (Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response

**Table A.296: Supported headers within the SUBSCRIBE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 3 | Retry-After | [26] 20.33 | m | m | [26] 20.33 | i | i |

**Table A.297: Void**

Prerequisite A.163/21 - - SUBSCRIBE response

Prerequisite: A.164/20 - - Additional for 407 (Proxy Authentication Required) response

**Table A.298: Supported headers within the SUBSCRIBE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 2 | Proxy-Authenticate | [26] 20.27 | m | m | [26] 20.27 | m | m |
| 6 | WWW-Authenticate | [26] 20.44 | m | m | [26] 20.44 | i | i |

Prerequisite A.163/21 - - SUBSCRIBE response

Prerequisite: A.164/25 - - Additional for 415 (Unsupported Media Type) response

**Table A.299: Supported headers within the SUBSCRIBE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Accept | [26] 20.1 | m | m | [26] 20.1 | i | i |
| 2 | Accept-Encoding | [26] 20.2 | m | m | [26] 20.2 | i | i |
| 3 | Accept-Language | [26] 20.3 | m | m | [26] 20.3 | i | i |

Prerequisite A.163/21 - - SUBSCRIBE response

Prerequisite: A.164/27 - - Additional for 420 (Bad Extension) response

**Table A.300: Supported headers within the SUBSCRIBE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 5 | Unsupported | [26] 20.40 | m | m | [26] 20.40 | c3 | c3 |
| c3: | IF A.162/18 THEN m ELSE i - - reading the contents of the Unsupported header before proxying the 420 response to a method other than REGISTER. | | | | | | |

Prerequisite A.163/21 - - SUBSCRIBE response

Prerequisite: A.164/28 OR A.164/41A - - Additional for 421 (Extension Required), 494 (Security Agreement Required) response

**Table A.300A: Supported headers within the SUBSCRIBE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 3 | Security-Server | [48] 2 | c1 | c1 | [48] 2 | n/a | n/a |
| c1: | IF A.162/47 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. | | | | | | |

Prerequisite A.163/21 - - SUBSCRIBE response

Prerequisite: A.164/29 - - Additional for 423 (Interval Too Brief) response

**Table A.301: Supported headers within the SUBSCRIBE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 2 | Min-Expires | [26] 20.23 | m | m | [26] 20.23 | i | i |

**Table A.302: Void**

Prerequisite A.163/21 - - SUBSCRIBE response

Prerequisite: A.164/39 - - Additional for 489 (Bad Event) response

**Table A.303: Supported headers within the SUBSCRIBE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Allow-Events | [28] 7.2.2 | m | m | [28] 7.2.2 | c1 | c1 |
| c1: | IF A.4/20 THEN m ELSE i - - SIP specific event notification extension. | | | | | | |
| NOTE: | c1 refers to the UA role major capability as this is the case of a proxy that also acts as a UA specifically for SUBSCRIBE and NOTIFY. | | | | | | |

**Table A.303A: Void**

Prerequisite A.163/21 - - SUBSCRIBE response

**Table A.304: Supported message bodies within the SUBSCRIBE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | | | | | | | |

### A.2.2.4.14 UPDATE method

Prerequisite A.163/22 - - UPDATE request

**Table A.305: Supported headers within the UPDATE request**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Accept | [26] 20.1 | m | m | [26] 20.1 | i | i |
| 1A | Accept-Contact | [56B] 9.2 | c21 | c21 | [56B] 9.2 | c22 | c22 |
| 2 | Accept-Encoding | [26] 20.2 | m | m | [26] 20.2 | i | i |
| 3 | Accept-Language | [26] 20.3 | m | m | [26] 20.3 | i | i |
| 4 | Allow | [26] 20.5 | m | m | [26] 20.5 | i | i |
| 5 | Allow-Events | [28] 7.2.2 | m | m | [28] 7.2.2 | c1 | c1 |
| 6 | Authorization | [26] 20.7 | m | m | [26] 20.7 | i | i |
| 7 | Call-ID | [26] 20.8 | m | m | [26] 20.8 | m | m |
| 8 | Call-Info | [26] 20.9 | m | m | [26] 20.9 | c8 | c8 |
| 9 | Contact | [26] 20.10 | m | m | [26] 20.10 | i | i |
| 10 | Content-Disposition | [26] 20.11 | m | m | [26] 20.11 | c4 | c4 |
| 11 | Content-Encoding | [26] 20.12 | m | m | [26] 20.12 | c4 | c4 |
| 12 | Content-Language | [26] 20.13 | m | m | [26] 20.13 | c4 | c4 |
| 13 | Content-Length | [26] 20.14 | m | m | [26] 20.14 | m | m |
| 14 | Content-Type | [26] 20.15 | m | m | [26] 20.15 | c4 | c4 |
| 15 | Cseq | [26] 20.16 | m | m | [26] 20.16 | m | m |
| 16 | Date | [26] 20.17 | m | m | [26] 20.17 | c2 | c2 |
| 17 | From | [26] 20.20 | m | m | [26] 20.20 | m | m |
| 18 | Max-Forwards | [26] 20.22 | m | m | [26] 20.22 | m | m |
| 19 | MIME-Version | [26] 20.24 | m | m | [26] 20.24 | i | c4 |
| 19A | Min-SE | [58] 5 | c23 | c23 | [58] 5 | c23 | c23 |
| 20 | Organization | [26] 20.25 | m | m | [26] 20.25 | c3 | c3 |
| 20A | P-Access-Network-Info | [52] 4.4 | c16 | c16 | [52] 4.4 | c17 | c17 |
| 20B | P-Charging-Function-Addresses | [52] 4.5 | c14 | c14 | [52] 4.5 | c15 | c15 |
| 20C | P-Charging-Vector | [52] 4.6 | c12 | c12 | [52] 4.6 | c13 | c13 |
| 20D | Privacy | [33] 4.2 | c10 | c10 | [33] 4.2 | c11 | c11 |
| 21 | Proxy-Authorization | [26] 20.28 | m | m | [26] 20.28 | c9 | c9 |
| 22 | Proxy-Require | [26] 20.29 | m | m | [26] 20.29 | m | m |
| 22A | Reason | [34A] 2 | c19 | c19 | [34A] 2 | c20 | c20 |
| 23 | Record-Route | [26] 20.30 | m | m | [26] 20.30 | c7 | c7 |
| 23A | Referred-By | [59] 3 | c24 | c24 | [59] 3 | c25 | c25 |
| 23B | Reject-Contact | [56B] 9.2 | c21 | c21 | [56B] 9.2 | c22 | c22 |
| 23C | Request-Disposition | [56B] 9.1 | c21 | c21 | [56B] 9.1 | c22 | c22 |
| 24 | Require | [26] 20.32 | m | m | [26] 20.32 | c5 | c5 |
| 25 | Route | [26] 20.34 | m | m | [26] 20.34 | m | m |
| 25A | Security-Client | [48] 2.3.1 | x | x | [48] 2.3.1 | c18 | c18 |
| 25B | Security-Verify | [48] 2.3.1 | x | x | [48] 2.3.1 | c18 | c18 |
| 25C | Session-Expires | [58] 4 | c23 | c23 | [58] 4 | c23 | c23 |
| 26 | Supported | [26] 20.37 | m | m | [26] 20.37 | c6 | c6 |
| 27 | Timestamp | [26] 20.38 | m | m | [26] 20.38 | i | i |
| 28 | To | [26] 20.39 | m | m | [26] 20.39 | m | m |
| 29 | User-Agent | [26] 20.41 | m | m | [26] 20.41 | i | i |
| 30 | Via | [26] 20.42 | m | m | [26] 20.42 | m | m |

| | |
|---|---|
| c1: | IF A.4/20 THEN m ELSE i - - SIP specific event notification extension. |
| c2: | IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses. |
| c3: | IF A.162/19A OR A.162/19B THEN m ELSE i - - reading, adding or concatenating the Organization header. |
| c4: | IF A.3/2 OR A.3/4 THEN m ELSE i - - P-CSCF or S-CSCF. |
| c5: | IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER. |
| c6: | IF A.162/16 THEN m ELSE i - - reading the contents of the Supported header before proxying the response. |
| c7: | IF A.162/14 THEN o ELSE i - - the requirement to be able to insert itself in the subsequent transactions in a dialog. |
| c8: | IF A.162/19C OR A.162/19D THEN m ELSE i - - reading, adding or concatenating the Call-Info header. |
| c9: | IF A.162/8A THEN m ELSE i - - authentication between UA and proxy. |
| c10: | IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP). |
| c11: | IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently. |
| c12: | IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension. |
| c13: | IF A.162/46 THEN m ELSE IF A.162/45 THEN i ELSE n/a - - adding, deleting, reading or modifying the P-Charging-Vector header before proxying the request or response or the P-Charging-Vector header extension. |
| c14: | IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension. |
| c15: | IF A.162/44A THEN m ELSE IF A.162/44 THEN i ELSE n/a - - adding, deleting or reading the P-Charging-Function-Addresses header before proxying the request or response, or the P-Charging-Function-Addresses header extension. |
| c16: | IF A.162/43 THEN x ELSE IF A.162/41 THEN m ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension. |
| c17: | IF A.162/43 THEN m ELSE IF A.162/41 THEN i ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension. |
| c18: | IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. |
| c19: | IF A.162/48 THEN m ELSE n/a - - the Reason header field for the session initiation protocol. |
| c20: | IF A.162/48 THEN i ELSE n/a - - the Reason header field for the session initiation protocol. |
| c21: | IF A.162/50 THEN m ELSE n/a - - caller preferences for the session initiation protocol. |
| c22: | IF A.162/50 THEN i ELSE n/a - - caller preferences for the session initiation protocol. |
| c23: | IF A.162/52 THEN m ELSE n/a - - the SIP session timer. |
| c24: | IF A.162/53 THEN i ELSE n/a - - the SIP Referred-By mechanism. |
| c25: | IF A.162/53 THEN m ELSE n/a - - the SIP Referred-By mechanism. |
| NOTE: | c1 refers to the UA role major capability as this is the case of a proxy that also acts as a UA specifically for SUBSCRIBE and NOTIFY. |

Prerequisite A.163/22 - - UPDATE request

**Table A.306: Supported message bodies within the UPDATE request**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | | | | | | | |

Prerequisite A.163/22 - - UPDATE response for all status-codes

**Table A.307: Supported headers within the UPDATE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 0A | Allow | [26] 20.5 | m | m | [26] 20.5 | i | i |
| 1 | Call-ID | [26] 20.8 | m | m | [26] 20.8 | m | m |
| 1A | Call-Info | [26] 20.9 | m | m | [26] 20.9 | c4 | c4 |
| 1B | Contact | [26] 20.10 | m | m | [26] 20.10 | i | i |
| 2 | Content-Disposition | [26] 20.11 | m | m | [26] 20.11 | i | c3 |
| 3 | Content-Encoding | [26] 20.12 | m | m | [26] 20.12 | i | c3 |
| 4 | Content-Language | [26] 20.13 | m | m | [26] 20.13 | i | c3 |
| 5 | Content-Length | [26] 20.14 | m | m | [26] 20.14 | m | m |
| 6 | Content-Type | [26] 20.15 | m | m | [26] 20.15 | i | c3 |
| 7 | Cseq | [26] 20.16 | m | m | [26] 20.16 | m | m |
| 8 | Date | [26] 20.17 | m | m | [26] 20.17 | c1 | c1 |
| 9 | From | [26] 20.20 | m | m | [26] 20.20 | m | m |
| 10 | MIME-Version | [26] 20.24 | m | m | [26] 20.24 | i | c3 |
| 10A | Organization | [26] 20.25 | m | m | [26] 20.25 | c2 | c2 |
| 10B | P-Access-Network-Info | [52] 4.4 | c11 | c11 | [52] 4.4 | c12 | c12 |
| 10C | P-Charging-Function-Addresses | [52] 4.5 | c9 | c9 | [52] 4.5 | c10 | c10 |
| 10D | P-Charging-Vector | [52] 4.6 | c7 | n/a | [52] 4.6 | c8 | n/a |
| 10E | Privacy | [33] 4.2 | c5 | c5 | [33] 4.2 | c6 | c6 |
| 10F | Require | [26] 20.32 | m | m | [26] 20.32 | c13 | c13 |
| 10G | Server | [26] 20.35 | m | m | [26] 20.35 | i | i |
| 11 | Timestamp | [26] 20.38 | m | m | [26] 20.38 | i | i |
| 12 | To | [26] 20.39 | m | m | [26] 20.39 | m | m |
| 12A | User-Agent | [26] 20.41 | m | m | [26] 20.41 | i | i |
| 13 | Via | [26] 20.42 | m | m | [26] 20.42 | m | m |
| 14 | Warning | [26] 20.43 | m | m | [26] 20.43 | i | i |
| c1: | IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses. | | | | | | |
| c2: | IF A.162/19A OR A.162/19B THEN m ELSE i - - reading, adding or concatenating the Organization header. | | | | | | |
| c3: | IF A.3/2 OR A.3/4 THEN m ELSE i - - P-CSCF or S-CSCF. | | | | | | |
| c4: | IF A.162/19C OR A.162/19D THEN m ELSE i - - reading, adding or concatenating the Call-Info header. | | | | | | |
| c5: | IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP). | | | | | | |
| c6: | IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently. | | | | | | |
| c7: | IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension. | | | | | | |
| c8: | IF A.162/46 THEN m ELSE IF A.162/45 THEN i ELSE n/a - - adding, deleting, reading or modifying the P-Charging-Vector header before proxying the request or response or the P-Charging-Vector header extension. | | | | | | |
| c9: | IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension. | | | | | | |
| c10: | IF A.162/44A THEN m ELSE IF A.162/44 THEN i ELSE n/a - - adding, deleting or reading the P-Charging-Function-Addresses header before proxying the request or response, or the P-Charging-Function-Addresses header extension. | | | | | | |
| c11: | IF A.162/43 THEN x ELSE IF A.162/41 THEN m ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension. | | | | | | |
| c12: | IF A.162/43 THEN m ELSE IF A.162/41 THEN i ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension. | | | | | | |
| c13: | IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER. | | | | | | |

Prerequisite A.163/23 - - UPDATE response

Prerequisite: A.164/102 - - Additional for 2xx response

**Table A.308: Supported headers within the UPDATE response**

| Item | Header | Sending | Receiving |
|---|---|---|---|

| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
|---|---|---|---|---|---|---|---|
| 0A | Accept | [26] 20.1 | m | m | [26] 20.1 | i | i |
| 0B | Accept-Encoding | [26] 20.2 | m | m | [26] 20.2 | i | i |
| 0C | Accept-Language | [26] 20.3 | m | m | [26] 20.3 | i | i |
| 1 | Allow-Events | [28] 7.2.2 | m | m | [28] 7.2.2 | c1 | c1 |
| 2 | Authentication-Info | [26] 20.6 | m | m | [26] 20.6 | i | i |
| 3 | Contact | [26] 20.10 | m | m | [26] 20.10 | i | i |
| 4 | Session-Expires | [58] 4 | c4 | c4 | [58] 4 | c4 | c4 |
| 6 | Supported | [26] 20.37 | m | m | [26] 20.37 | i | i |
| c1: | IF A.4/20 THEN m ELSE i - - SIP specific event notification extension. | | | | | | |
| c3: | IF A.162/15 THEN o ELSE i - - the requirement to be able to use separate URIs in the upstream direction and downstream direction when record routeing. | | | | | | |
| c4: | IF A.162/52 THEN m ELSE n/a - - the SIP session timer | | | | | | |

Prerequisite A.163/23 - - UPDATE response

Prerequisite: A.164/103 OR A.164/104 OR A.164/105 OR A.164/106 - - Additional for 3xx – 6xx response

**Table A.308A: Supported headers within the UPDATE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Error-Info | [26] 20.18 | m | m | [26] 20.18 | i | i |

Prerequisite A.163/23 - - UPDATE response

Prerequisite: A.164/103 or A.164/35 - - Additional for 3xx, 485 (Ambiguous) response

**Table A.309: Supported headers within the UPDATE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 2 | Contact | [26] 20.10 | m | m | [26] 20.10 | c1 | c1 |
| c1: | IF A.162/19E THEN m ELSE i - - deleting Contact headers. | | | | | | |

Prerequisite A.163/23 - - UPDATE response

Prerequisite: A.164/14 - - Additional for 401 (Unauthorized) response

**Table A.309A: Supported headers within the UPDATE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 3 | Proxy-Authenticate | [26] 20.27 | m | m | [26] 20.27 | m | m |
| 6 | WWW-Authenticate | [26] 20.44 | m | m | [26] 20.44 | i | i |

Prerequisite A.163/23 - - UPDATE response

Prerequisite: A.164/17 OR A.164/23 OR A.164/30 OR A.164/36 OR A.164/42 OR A.164/45 OR A.164/50 OR A.164/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response

**Table A.310: Supported headers within the UPDATE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 5 | Retry-After | [26] 20.33 | m | m | [26] 20.33 | i | i |

**Table A.311: Void**

Prerequisite A.163/23 - - UPDATE response

Prerequisite: A.164/20 - - Additional for 407 (Proxy Authentication Required) response

**Table A.312: Supported headers within the UPDATE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 4 | Proxy-Authenticate | [26] 20.27 | m | m | [26] 20.27 | m | m |
| 8 | WWW-Authenticate | [26] 20.44 | m | m | [26] 20.44 | i | i |

Prerequisite A.163/23 - - UPDATE response

Prerequisite: A.164/25 - - Additional for 415 (Unsupported Media Type) response

**Table A.313: Supported headers within the UPDATE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Accept | [26] 20.1 | m | m | [26] 20.1 | i | i |
| 2 | Accept-Encoding | [26] 20.2 | m | m | [26] 20.2 | i | i |
| 3 | Accept-Language | [26] 20.3 | m | m | [26] 20.3 | i | i |

Prerequisite A.163/23 - - UPDATE response

Prerequisite: A.164/27 - - Additional for 420 (Bad Extension) response

**Table A.314: Supported headers within the UPDATE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 7 | Unsupported | [26] 20.40 | m | m | [26] 20.40 | c3 | c3 |
| c3: | IF A.162/18 THEN m ELSE i - - reading the contents of the Unsupported header before proxying the 420 response to a method other than REGISTER. | | | | | | |

Prerequisite A.163/23 - - UPDATE response

Prerequisite: A.164/28 OR A.164/41A - - Additional for 421 (Extension Required), 494 (Security Agreement Required) response

**Table A.314A: Supported headers within the UPDATE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 3 | Security-Server | [48] 2 | c1 | c1 | [48] 2 | n/a | n/a |
| c1: | IF A.162/47 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. | | | | | | |

Prerequisite A.163/23 - - UPDATE response

Prerequisite: A.164/28A - - Additional for 422 (Session Interval Too Small) response

**Table A.314B: Supported headers within the UPDATE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Min-SE | [58] 5 | c1 | c1 | [58] 5 | c1 | c1 |
| c1: | IF A.162/52 THEN m ELSE n/a - - the SIP session timer. | | | | | | |

**Table A.315: Void**

Prerequisite A.163/23 - - UPDATE response

**Table A.316: Supported message bodies within the UPDATE response**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | | | | | | | |

# A.3 Profile definition for the Session Description Protocol as used in the present document

## A.3.1 Introduction

Void.

## A.3.2 User agent role

This subclause contains the ICS proforma tables related to the user agent role. They need to be completed only for UA implementations.

Prerequisite: A.2/1 -- user agent role

### A.3.2.1 Major capabilities

**Table A.317: Major capabilities**

| Item | Does the implementation support | Reference | RFC status | Profile status |
|---|---|---|---|---|
| | **Capabilities within main protocol** | | | |
| | | | | |
| | **Extensions** | | | |
| 22 | Integration of resource management and SIP? | [30] [64] | o | m |
| 23 | Grouping of media lines | [53] | o | c1 |
| 24 | Mapping of Media Streams to Resource Reservation Flows | [54] | o | c1 |
| 25 | SDP Bandwidth Modifiers for RTCP Bandwidth | [56] | o | o (NOTE 1) |
| c1: IF A.3/1 THEN m ELSE n/a - - UE role.<br>NOTE 1: For "video" and "audio" media types that utilise RTP/RTCP, it shall be specified. For other media types, it may be specified. | | | | |

### A.3.2.2 SDP types

**Table A.318: SDP types**

| Item | Type | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| | **Session level description** | | | | | | |
| 1 | v= (protocol version) | [39] 5.1 | m | m | [39] 5.1 | m | m |
| 2 | o= (owner/creator and session identifier) | [39] 5.2 | m | m | [39] 5.2 | m | m |
| 3 | s= (session name) | [39] 5.3 | m | m | [39] 5.3 | m | m |
| 4 | i= (session information) | [39] 5.4 | o | o | [39] 5.4 | m | m |
| 5 | u= (URI of description) | [39] 5.5 | o | n/a | [39] 5.5 | o | n/a |
| 6 | e= (email address) | [39] 5.6 | o | n/a | [39] 5.6 | o | n/a |
| 7 | p= (phone number) | [39] 5.6 | o | n/a | [39] 5.6 | o | n/a |
| 8 | c= (connection information) | [39] 5.7 | o | o | [39] 5.7 | m | m |
| 9 | b= (bandwidth information) | [39] 5.8 | o | o (NOTE 1) | [39] 5.8 | m | m |
| | **Time description (one or more per description)** | | | | | | |
| 10 | t= (time the session is active) | [39] 5.9 | m | m | [39] 5.9 | m | m |
| 11 | r= (zero or more repeat times) | [39] 5.10 | o | n/a | [39] 5.10 | o | n/a |
| | **Session level description (continued)** | | | | | | |
| 12 | z= (time zone adjustments) | [39] 5.11 | o | n/a | [39] 5.11 | o | n/a |
| 13 | k= (encryption key) | [39] 5.12 | o | o | [39] 5.12 | o | o |
| 14 | a= (zero or more session attribute lines) | [39] 5.13 | o | o | [39] 5.13 | m | m |
| | **Media description (zero or more per description)** | | | | | | |
| 15 | m= (media name and transport address) | [39] 5.14 | o | o | [39] 5.14 | m | m |
| 16 | i= (media title) | [39] 5.4 | o | o | [39] 5.4 | o | o |
| 17 | c= (connection information) | [39] 5.7 | c1 | c1 | [39] 5.7 | c1 | c1 |
| 18 | b= (bandwidth information) | [39] 5.8 | o | o (NOTE 1) | [39] 5.8 | | |
| 19 | k= (encryption key) | [39] 5.12 | o | o | [39] 5.12 | o | o |
| 20 | a= (zero or more media attribute lines) | [39] 5.13 | o | o | [39] 5.13 | m | m |
| c1: IF A.318/15 THEN m ELSE n/a.<br>NOTE 1: For "video" and "audio" media types that utilise RTP/RTCP, it shall be specified. For other media types, it may be specified. | | | | | | | |

Prerequisite A.318/14 OR A.318/20 - - a= (zero or more session/media attribute lines)

**Table A.319: zero or more session / media attribute lines (a=)**

| Item | Field | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | category (a=cat) | [39] 6 | | | [39] 6 | | |
| 2 | keywords (a=keywds) | [39] 6 | | | [39] 6 | | |
| 3 | name and version of tool (a=tool) | [39] 6 | | | [39] 6 | | |
| 4 | packet time (a=ptime) | [39] 6 | | | [39] 6 | | |
| 5 | maximum packet time (a=maxptime) | [39] 6 | | | [39] 6 | | |
| 6 | receive-only mode (a=recvonly) | [39] 6 | | | [39] 6 | | |
| 7 | send and receive mode (a=sendrecv) | [39] 6 | | | [39] 6 | | |
| 8 | send-only mode (a=sendonly) | [39] 6 | | | [39] 6 | | |
| 9 | whiteboard orientation (a=orient) | [39] 6 | | | [39] 6 | | |
| 10 | conference type (a=type) | [39] 6 | | | [39] 6 | | |
| 11 | character set (a=charset) | [39] 6 | | | [39] 6 | | |
| 12 | language tag (a=sdplang) | [39] 6 | | | [39] 6 | | |
| 13 | language tag (a=lang) | [39] 6 | | | [39] 6 | | |
| 14 | frame rate (a=framerate) | [39] 6 | | | [39] 6 | | |
| 15 | quality (a=quality) | [39] 6 | | | [39] 6 | | |
| 16 | format specific parameters (a=fmtp) | [39] 6 | | | [39] 6 | | |
| 17 | rtpmap attribute (a=rtpmap) | [39] 6 | | | [39] 6 | | |
| 18 | current-status attribute (a=curr) | [30] 5 | c1 | c1 | [30] 5 | c2 | c2 |
| 19 | desired-status attribute (a=des) | [30] 5 | c1 | c1 | [30] 5 | c2 | c2 |
| 20 | confirm-status attribute (a=conf) | [30] 5 | c1 | c1 | [30] 5 | c2 | c2 |
| 21 | media stream identification attribute (a=mid) | [53] 3 | c3 | c3 | [53] 3 | c4 | c4 |
| 22 | group attribute (a=group) | [53] 4 | c5 | c5 | [53] 3 | c6 | c6 |
| c1: | IF A.317/22 THEN o ELSE n/a. | | | | | | |
| c2: | IF A.317/22 THEN m ELSE n/a. | | | | | | |
| c3: | IF A.317/23 THEN o ELSE n/a. | | | | | | |
| c4: | IF A.317/23 THEN m ELSE n/a. | | | | | | |
| c5: | IF A.317/24 THEN o ELSE n/a. | | | | | | |
| c6: | IF A.317/24 THEN m ELSE n/a. | | | | | | |

### A.3.2.3 Void

**Table A.320: Void**

**Table A.321: Void**

**Table A.322: Void**

**Table A.323: Void**

**Table A.324: Void**

**Table A.325: Void**

**Table A.326: Void**

**Table A.327: Void**

### A.3.2.4 Void

**Table A.327A: Void**

## A.3.3 Proxy role

This subclause contains the ICS proforma tables related to the user role. They need to be completed only for proxy implementations.

Prerequisite: A.2/2 -- proxy role

### A.3.3.1 Major capabilities

**Table A.328: Major capabilities**

| Item | Does the implementation support | Reference | RFC status | Profile status |
|---|---|---|---|---|
| | **Capabilities within main protocol** | | | |
| | | | | |
| | **Extensions** | | | |
| 1 | Integration of resource management and SIP? | [30] [64] | o | n/a |
| 2 | Grouping of media lines | [53] | o | c1 |
| 3 | Mapping of Media Streams to Resource Reservation Flows | [54] | o | c1 |
| 4 | SDP Bandwidth Modifiers for RTCP Bandwidth | [56] | o | c1 |
| c1: IF A.3/2 THEN m ELSE n/a - - P-CSCF role. | | | | |

## A.3.3.2 SDP types

**Table A.329: SDP types**

| Item | Type | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| | **Session level description** | | | | | | |
| 1 | v= (protocol version) | [39] 5.1 | m | m | [39] 5.1 | m | m |
| 2 | o= (owner/creator and session identifier). | [39] 5.2 | m | m | [39] 5.2 | i | i |
| 3 | s= (session name) | [39] 5.3 | m | m | [39] 5.3 | i | i |
| 4 | i= (session information) | [39] 5.4 | m | m | [39] 5.4 | i | i |
| 5 | u= (URI of description) | [39] 5.5 | m | m | [39] 5.5 | i | i |
| 6 | e= (email address) | [39] 5.6 | m | m | [39] 5.6 | i | i |
| 7 | p= (phone number) | [39] 5.6 | m | m | [39] 5.6 | i | i |
| 8 | c= (connection information) | [39] 5.7 | m | m | [39] 5.7 | i | i |
| 9 | b= (bandwidth information) | [39] 5.8 | m | m | [39] 5.8 | i | i |
| | **Time description (one or more per description)** | | | | | | |
| 10 | t= (time the session is active) | [39] 5.9 | m | m | [39] 5.9 | i | i |
| 11 | r= (zero or more repeat times) | [39] 5.10 | m | m | [39] 5.10 | i | i |
| | **Session level description (continued)** | | | | | | |
| 12 | z= (time zone adjustments) | [39] 5.11 | m | m | [39] 5.11 | i | i |
| 13 | k= (encryption key) | [39] 5.12 | m | m | [39] 5.12 | i | i |
| 14 | a= (zero or more session attribute lines) | [39] 5.13 | m | m | [39] 5.13 | i | i |
| | **Media description (zero or more per description)** | | | | | | |
| 15 | m= (media name and transport address) | [39] 5.14 | m | m | [39] 5.14 | m | m |
| 16 | i= (media title) | [39] 5.4 | o | | [39] 5.4 | | |
| 17 | c= (connection information) | [39] 5.7 | o | | [39] 5.7 | | |
| 18 | b= (bandwidth information) | [39] 5.8 | o | | [39] 5.8 | | |
| 19 | k= (encryption key) | [39] 5.12 | o | | [39] 5.12 | | |
| 20 | a= (zero or more media attribute lines) | [39] 5.13 | o | | [39] 5.13 | | |

Prerequisite A.329/14 OR A.329/20 - - a= (zero or more session/media attribute lines)

**Table A.330: zero or more session / media attribute lines (a=)**

| Item | Field | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | category (a=cat) | [39] 6 | | | [39] 6 | | |
| 2 | keywords (a=keywds) | [39] 6 | | | [39] 6 | | |
| 3 | name and version of tool (a=tool) | [39] 6 | | | [39] 6 | | |
| 4 | packet time (a=ptime) | [39] 6 | | | [39] 6 | | |
| 5 | maximum packet time (a=maxptime) | [39] 6 | | | [39] 6 | | |
| 6 | receive-only mode (a=recvonly) | [39] 6 | | | [39] 6 | | |
| 7 | send and receive mode (a=sendrecv) | [39] 6 | | | [39] 6 | | |
| 8 | send-only mode (a=sendonly) | [39] 6 | | | [39] 6 | | |
| 9 | whiteboard orientation (a=orient) | [39] 6 | | | [39] 6 | | |
| 10 | conference type (a=type) | [39] 6 | | | [39] 6 | | |
| 11 | character set (a=charset) | [39] 6 | | | [39] 6 | | |
| 12 | language tag (a=sdplang) | [39] 6 | | | [39] 6 | | |
| 13 | language tag (a=lang) | [39] 6 | | | [39] 6 | | |
| 14 | frame rate (a=framerate) | [39] 6 | | | [39] 6 | | |
| 15 | quality (a=quality) | [39] 6 | | | [39] 6 | | |
| 16 | format specific parameters (a=fmtp) | [39] 6 | | | [39] 6 | | |
| 17 | rtpmap attribute (a=rtpmap) | [39] 6 | | | [39] 6 | | |
| 18 | current-status attribute (a=curr) | [30] 5 | m | m | [30] 5 | c2 | c2 |
| 19 | desired-status attribute (a=des) | [30] 5 | m | m | [30] 5 | c2 | c2 |
| 20 | confirm-status attribute (a=conf) | [30] 5 | m | m | [30] 5 | c2 | c2 |
| 21 | media stream identification attribute (a=mid) | [53] 3 | c3 | c3 | [53] 3 | c4 | c4 |
| 22 | group attribute (a=group) | [53] 4 | c5 | c6 | [53] 3 | c5 | c6 |
| c2: | IF A.328/1 THEN m ELSE i. | | | | | | |
| c3: | IF A.328/2 THEN o ELSE n/a. | | | | | | |
| c4: | IF A.328/2 THEN m ELSE n/a. | | | | | | |
| c5: | IF A.328/3 THEN o ELSE n/a. | | | | | | |
| c6: | IF A.328/3 THEN m ELSE n/a. | | | | | | |

### A.3.3.3 Void

**Table A.331: Void**

**Table A.332: Void**

**Table A.333: Void**

**Table A.334: Void**

**Table A.335: Void**

**Table A.336: Void**

**Table A.337: Void**

**Table A.338: Void**

### A.3.3.4 Void

**Table A.339: Void**

## A.4 Profile definition for other message bodies as used in the present document

Void.

# Annex B (normative): IP-Connectivity Access Network specific concepts when using GPRS to access IM CN subsystem

## B.1 Scope

The present annex defines IP-CAN specific requirements for a call control protocol for use in the IP Multimedia (IM) Core Network (CN) subsystem based on the Session Initiation Protocol (SIP), and the associated Session Description Protocol (SDP), where the IP-CAN is General Packet Radio Service (GPRS).

## B.2 GPRS aspects when connected to the IM CN subsystem

### B.2.1 Introduction

A UE accessing the IM CN subsystem, and the IM CN subsystem itself, utilise the services provided by GPRS to provide packet-mode communication between the UE and the IM CN subsystem.

Requirements for the UE on the use of these packet-mode services are specified in this clause. Requirements for the GGSN in support of this communication are specified in 3GPP TS 29.061 [11] and 3GPP TS 29.207 [12].

When using the GPRS, each IP-CAN bearer is provided by a PDP context.

### B.2.2 Procedures at the UE

#### B.2.2.1 PDP context activation and P-CSCF discovery

Prior to communication with the IM CN subsystem, the UE shall:

a) perform a GPRS attach procedure;

b) establish a PDP context used for SIP signalling according to the APN and GGSN selection criteria described in 3GPP TS 23.060 [4] and 3GPP TS 27.060 [10A]. This PDP context shall remain active throughout the period the UE is connected to the IM CN subsystem, i.e. from the initial registration and at least until the deregistration. As a result, the PDP context provides the UE with information that makes the UE able to construct an IPv6 address;

   The UE shall choose one of the following options when performing establishment of this PDP context:

   I. A dedicated PDP context for SIP signalling:

      The UE shall indicate to the GGSN that this is a PDP context intended to carry IM CN subsystem-related signalling only by setting the IM CN Subsystem Signalling Flag. The UE may also use this PDP context for DNS and DHCP signalling according to the static packet filters as described in 3GPP TS 29.061 [11]. The UE can also set the Signalling Indication attribute within the QoS IE;

   II. A general-purpose PDP context:

      The UE may decide to use a general-purpose PDP Context to carry IM CN subsystem-related signaling. The UE shall indicate to the GGSN that this is a general-purpose PDP context by not setting the IM CN Subsystem Signalling Flag. The UE may carry both signalling and media on the general-purpose PDP context. The UE can also set the Signalling Indication attribute within the QoS IE.

The UE indicates the IM CN Subsystem Signalling Flag to the GGSN within the Protocol Configuration Options IE of the ACTIVATE PDP CONTEXT REQUEST message or ACTIVATE SECONDARY PDP CONTEXT REQUEST message. Upon successful signalling PDP context establishment the UE receives an indication from GGSN in the form of IM CN Subsystem Signalling Flag within the Protocol Configuration Options IE. If the flag is not received, the UE shall consider the PDP context as a general-purpose PDP context.

The encoding of the IM CN Subsystem Signalling Flag within the Protocol Configuration Options IE is described in 3GPP TS 24.008 [8].

The UE can indicate a request for prioritised handling over the radio interface by setting the Signalling Indication attribute (see 3GPP TS 23.107 [4A]). The general QoS negotiation mechanism and the encoding of the Signalling Indication attribute within the QoS IE are described in 3GPP TS 24.008 [8].

NOTE: A general-purpose PDP Context may carry both IM CN subsystem signaling and media, in case the media does not need to be authorized by Service Based Local Policy mechanisms defined in 3GPP TS 29.207 [12] and the media stream is not mandated by the P-CSCF to be carried in a separate PDP Context.

c) acquire a P-CSCF address(es).

The methods for P-CSCF discovery are:

I. Employ Dynamic Host Configuration Protocol for IPv6 (DHCPv6) RFC 3315 [40], the DHCPv6 options for SIP servers RFC 3319 [41] and DHCPv6 options for Domain Name Servers (DNS) RFC 3646 [56C] as described in subclause 9.2.1.

II. Transfer P-CSCF address(es) within the PDP context activation procedure.

The UE shall indicate the request for a P-CSCF address to the GGSN within the Protocol Configuration Options IE of the ACTIVATE PDP CONTEXT REQUEST message or ACTIVATE SECONDARY PDP CONTEXT REQUEST message.

If the GGSN provides the UE with a list of P-CSCF IPv6 addresses in the ACTIVATE PDP CONTEXT ACCEPT message or ACTIVATE SECONDARY PDP CONTEXT ACCEPT message, the UE shall assume that the list is prioritised with the first address within the Protocol Configuration Options IE as the P-CSCF address with the highest priority.

The UE can freely select method I or II for P-CSCF discovery. In case method I is selected and several P-CSCF addresses or FQDNs are provided to the UE, the selection of P-CSCF address or FQDN shall be performed as indicated in RFC 3319 [41]. If sufficient information for P-CSCF address selection is not available, selection of the P-CSCF address by the UE is implementation specific.

If the UE is designed to use I above, but receives P-CSCF address(es) according to II, then the UE shall either ignore the received address(es), or use the address(es) in accordance with II, and not proceed with the DHCP request according to I.

The UE may request a DNS Server IPv6 address(es) via RFC 3315 [40] and RFC 3646 [56C] or by the Protocol Configuration Options IE when activating a PDP context according to 3GPP TS 27.060 [10A].

The encoding of the request and response for IPv6 address(es) for DNS server(s) and list of P-CSCF address(es) within the Protocol Configuration Options IE is described in 3GPP TS 24.008 [8].

## B.2.2.1A Modification of a PDP context used for SIP signalling

The PDP context shall not be modified from a dedicated PDP context for SIP signalling to a general-purpose PDP context or vice versa. The IM CN Subsystem Signalling Flag shall not be set in the Protocol Configuration Options IE of the MODIFY PDP CONTEXT REQUEST message.

The UE shall not indicate the request for a P-CSCF address to the GGSN within the Protocol Configuration Options IE of the MODIFY PDP CONTEXT REQUEST message. The UE shall ignore P-CSCF address(es) if received from the GGSN in the Protocol Configuration Options IE of the MODIFY PDP CONTEXT RESPONSE message.

## B.2.2.1B Re-establishment of the PDP context for signalling

If the dedicated PDP context for SIP signalling is lost due to e.g. a GPRS routeing area update procedure, the UE shall attempt to re-establish the dedicated PDP context for SIP signalling. If this procedure does not succeed, the UE shall deactivate all PDP contexts established as a result of SIP signalling according to the 3GPP TS 24.008 [8].

## B.2.2.2 Session management procedures

The existing procedures for session management as described in 3GPP TS 24.008 [8] shall apply while the UE is connected to the IM CN subsystem.

## B.2.2.3 Mobility management procedures

The existing procedures for mobility management as described in 3GPP TS 24.008 [8] shall apply while the UE is connected to the IM CN subsystem.

## B.2.2.4 Cell selection and lack of coverage

The existing mechanisms and criteria for cell selection as described in 3GPP TS 25.304 [9] and 3GPP TS 44.018 [20] shall apply while the UE is connected to the IM CN subsystem.

## B.2.2.5 PDP contexts for media

### B.2.2.5.1 General requirements

The UE can establish media streams that belong to different SIP sessions on the same PDP context.

During establishment of a session, the UE establishes data streams(s) for media related to the session. Such data stream(s) may result in activation of additional PDP context(s). Such additional PDP context(s) shall be established as secondary PDP contexts associated to the PDP context used for signalling.

When the UE has to allocate bandwidth for RTP and RTCP in a PDP context, the UE shall use the rules outlined in 3GPP TS 29.208 [13].

### B.2.2.5.1A Activation or modification of PDP contexts for media

If the UE receives indication within the SDP according to RFC 3524 [54] that media stream(s) belong to group(s), the media stream(s) shall be set up on separate PDP contexts according to the indication of grouping of media streams. The UE may freely group media streams to PDP context(s) in case no indication of grouping of media streams is received from the P-CSCF.

If the capabilities of the originating UE prevents it from establishment of additional PDP contexts according to the media grouping attributes given by the P-CSCF in accordance with RFC 3524 [54], the UE will not establish such grouping of media streams. Instead, the originating UE shall negotiate media parameters for the session according to RFC 3264 [27B].

If the capabilities of the terminating UE prevents it from establishment of additional PDP contexts according to the media grouping attributes given by the P-CSCF in accordance with RFC 3524 [54], the UE will not establish such grouping of media streams. Instead, the terminating UE shall the UE shall handle such SDP offers in accordance with RFC 3388 [53].

The UE can receive a media authorization token in the P-Media-Authorization header from the P-CSCF according to RFC 3313 [31]. If a media authorization token is received in the P-Media-Authorization header when a SIP session is initiated, the UE shall:

- either use existing PDP context(s) where another media authorization token is already in use and no indication of grouping of media streams is required; or
- establish separate PDP context(s) for the media; or

- use an existing PDP context where media authorization token is not in use and no indication of grouping of media streams is required.

When a UE modifies a PDP context to indicate a new media authorization token:

- either as a result of establishment of an additional SIP session; or
- modification of media streams for an ongoing SIP session;

the UE shall include all media authorization tokens and all flow identifiers for all ongoing SIP sessions that use this particular PDP context.

If a media authorization token is received in subsequent messages for the same SIP session, the UE shall:

- use the existing PDP context(s) for media;
- modify the existing PDP context(s) for media; or
- establish additional PDP context(s) for media.

If either background or interactive QoS class is needed for the media, then the UE does not need to use the authorization token even if it receives one. In this case the UE may reuse an existing PDP context and it does not need to request PDP context modification unless it needs to modify the QoS.

If existing PDP context(s) where another media authorization token is already in use is re-used for the media, or separate PDP context(s) is established for the media, the UE shall proceed as follows:

- when a SIP session is terminated, the media authorization token is no longer valid and the UE shall not include it in future GPRS session management messages. The UE shall send a MODIFY PDP CONTEXT REQUEST message updating the binding information by deleting the media authorization token and the corresponding flow identifiers that are no longer valid. If a SIP session is terminated and no other SIP sessions are using the PDP context, the UE shall either update the binding information as described above or deactivate the PDP context;
- the UE shall transparently pass the media authorization token received from the P-CSCF in a response to an INVITE request at originating setup or in the INVITE request at terminating setup to the GGSN. The UE shall signal it by inserting it within the Traffic Flow Template IE in the ACTIVATE SECONDARY PDP CONTEXT REQUEST message or the MODIFY PDP CONTEXT REQUEST message;
- to identify to the GGSN which flow(s) (identified by m-lines within the SDP) that are transferred within a particular PDP context, the UE shall set the flow identifier(s) within the Traffic Flow Template IE in the ACTIVATE SECONDARY PDP CONTEXT REQUEST message or the MODIFY PDP CONTEXT REQUEST message. Detailed description of how the flow identifiers are constructed is provided in 3GPP TS 29.207 [12];
- if the UE receives several media authorization tokens from the P-CSCF within the same SIP request or response, the first instance of the media authorization token shall be sent to the GGSN, and subsequent instances are discarded by the UE; and
- the UE shall not include the IM CN Subsystem Signalling Flag when a PDP context for media is established or modified.

The encoding of the media authorization token and the flow identifiers within the Traffic Flow Template IE is described in 3GPP TS 24.008 [8].

#### B.2.2.5.2 Special requirements applying to forked responses

Since the UE does not know that forking has occurred until a second, provisional response arrives, the UE sets up the PDP context(s) as required by the initial response received. If a subsequent provisional response is received, different alternative actions may be performed depending on the requirements in the SDP answer:

1) **the bearer requirements of the subsequent SDP can be accommodated by the existing PDP context(s).** The UE performs no activation or modification of PDP contexts.
2) **the subsequent SDP introduces different QoS requirements or additional IP flows.** The UE modifies the existing PDP context(s), if necessary, according to subclause B.2.2.5.1A.

3) **the subsequent SDP introduces one or more additional IP flows.** The UE establishes additional PDP context(s) according to subclause B.2.2.5.1A.

NOTE 1: When several forked responses are received, the resources requested by the UE is are the 'logical OR' of the resources indicated in the multiple responses to avoid allocation of unnecessary resources. The UE does not request more resources than proposed in the original INVITE request.

NOTE 2: When service-based local policy is applied, the UE receives the same authorization token for all forked requests/responses related to the same SIP session.

When a final answer is received for one of the early dialogues, the UE proceeds to set up the SIP session. The UE shall release all the unneeded radio/bearer resources. Therefore, upon the reception of a first final 200 (OK) response for the INVITE request (in addition to the procedures defined in RFC 3261 [26] subclause 13.2.2.4), the UE shall:

1) in case PDP context(s) were established or modified as a consequence of the INVITE request and forked provisional responses that are not related to the accepted 200 (OK) response, delete the PDP context(s) or modify the delete the PDP context(s) back to their original state.

#### B.2.2.5.3 Unsuccessful situations

One of the Go interface related error codes can be received by the UE in the ACTIVATE SECONDARY PDP CONTEXT REJECT message or the MODIFY PDP CONTEXT REJECT message. If the UE receives a Go interface related error code, the UE shall either terminate the session or retransmit the message up to three times. The Go interface related error codes are further specified in 3GPP TS 29.207 [12].

## B.3 Application usage of SIP

### B.3.1 Procedures at the UE

#### B.3.1.1 Void

## B.4 3GPP specific encoding for SIP header extensions

### B.4.1 Void

# Annex C (normative): UICC and USIM Aspects for access to the IM CN subsystem

## C.1 Scope

This clause describes the UICC and USIM aspects for access to the IM CN subsystem. Additional requirements related to UICC usage for access to the IM CN subsystem are described in 3GPP TS 33.203 [19].

## C.2 Derivation of IMS parameters from USIM

In case the UE is loaded with a UICC that contains a USIM application but does not contain an ISIM application, the UE shall:

- generate a private user identity;
- generate a temporary public user identity; and
- generate a home network domain name to address the SIP REGISTER request to.

All these three parameters are derived from the IMSI parameter in the USIM, according to the procedures described in 3GPP TS 23.003 [3]. Also in this case, the UE shall derive new values every time the UICC is changed, and shall discard existing values if the UICC is removed.

NOTE: If there is an ISIM and a USIM application on a UICC, the ISIM application is used for IMS authentication, as described in 3GPP TS 33.203 [19]. See subclause 5.1.1.1A.

## C.3 ISIM Location in 3GPP Systems

For 3GPP systems, if ISIM application is present, it is contained in UICC.

# Annex D (normative): IP-Connectivity Access Network specific concepts when using I-WLAN to access IM CN subsystem

## D.1 Scope

The present annex defines IP-CAN specific requirements for a call control protocol for use in the IP Multimedia (IM) Core Network (CN) subsystem based on the Session Initiation Protocol (SIP), and the associated Session Description Protocol (SDP), where the IP-CAN is Wireless LAN Interworking (I-WLAN).

## D.2 I-WLAN aspects when connected to the IM CN subsystem

### D.2.1 Introduction

A WLAN UE accessing the IM CN subsystem, and the IM CN subsystem itself, utilise the services provided by I-WLAN to provide packet-mode communication between the WLAN UE and the IM CN subsystem.

Requirements for the WLAN UE on the use of these packet-mode services are specified in this clause. Requirements for the PDG in support of this communication are specified in 3GPP TS 29.161 [11C]. When using the I-WLAN, the IP-CAN bearer is provided by an I-WLAN tunnel.

### D.2.2 Procedures at the WLAN UE

#### D.2.2.1 I-WLAN tunnel activation and P-CSCF discovery

Prior to communication with the IM CN subsystem, the WLAN UE shall:

a) Perform I-WLAN network selection i.e. gaining 3GPP Direct access as described in 3GPP TS 24.234 [8C] in the access dependent case;

b) Establish an IKE security association and an IPsec ESP security association (I-WLAN tunnel) with the PDG according to the W-APN and PDG selection criteria described in 3GPP TS 24.234 [8C]. The IKE security association and IPsec ESP security association (I-WLAN tunnel) shall remain active throughout the period the WLAN UE is connected to the IM CN subsystem, i.e. from the initial registration and at least until the deregistration.;

The WLAN UE may carry both signalling and media on an IPsec ESP security association.

c) Acquire a P-CSCF address(es).

The method for P-CSCF discovery is:

Employ Dynamic Host Configuration Protocol for IPv6 (DHCPv6) RFC 3315 [40], the DHCPv6 options for SIP servers RFC 3319 [41] and the DHCPv6 options for Domain Name Servers (DNS) RFC 3646 [56C] as described in subclause 9.2.1.

In case several P-CSCF addresses or FQDNs are provided to the UE, the selection of P-CSCF address or FQDN shall be performed as indicated in RFC 3319 [41]. If sufficient information for P-CSCF address selection is not available, selection of the P-CSCF address by the WLAN UE is implementation specific.

The WLAN UE may request a DNS Server IPv6 address(es) via RFC 3315 [40] and RFC 3646 [56C].

## D.2.2.2 I-WLAN tunnel procedures

### D.2.2.2.1 General requirements

The WLAN UE can establish media streams that belong to different SIP sessions on the same I-WLAN tunnel.

During establishment of a session, the WLAN UE establishes data streams(s) for media related to the session. Such data stream(s) may result in activation of additional IPsec ESP security association (I-WLAN tunnels).

### D.2.2.2.2 Usage of I-WLAN tunnel for media

If the WLAN UE receives indication within the SDP according to RFC 3524 [54] that media stream(s) belong to group(s), the media stream(s) shall be set up on separate IPSEC ESP security association (I-WLAN tunnels) according to the indication of grouping of media streams. The WLAN UE may freely group media streams to IPsec ESP security association (I-WLAN tunnel(s)) in case no indication of grouping of media streams is received from the P-CSCF.

If the capabilities of the originating WLAN UE, or operator policy at the PDG prevents the originating WLAN UE from establishment of additional IPsec ESP security association (I-WLAN tunnels) according to the media grouping attributes given by the P-CSCF in accordance with RFC 3524 [54], the WLAN UE will not establish such grouping of media streams. Instead, the originating WLAN UE shall negotiate media parameters for the session according to RFC 3264 [27B].

If the capabilities of the terminating WLAN UE or operator policy at the PDG prevents the originating WLAN UE from establishment of additional IPsec ESP security association (I-WLAN tunnels) according to the media grouping attributes given by the P-CSCF in accordance with RFC 3524 [54], the WLAN UE will not establish such grouping of media streams. Instead, the terminating WLAN UE shall handle such SDP offers in accordance with RFC 3388 [53].

The UE can receive a media authorization token in the P-Media-Authorization header from the P-CSCF according to RFC 3313 [31]. If a media authorization token is received in the P-Media-Authorization header when a SIP session is initiated, the UE shall reuse the existing I-WLAN tunnel and ignore the media authorization token.

### D.2.2.2.3 Special requirements applying to forked responses

Since the UE is unable to perform bearer modification, forked responses place no special requirements on the UE.

# Annex E (informative): Change history

| Change history | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Date | TSG # | TSG Doc. | CR | Rev | Subject/Comment | Old | New | WG doc |
| | | | | | Version 0.0.0 Editor's internal draft | | | |
| | | | | | Version 0.0.1 Editor's internal draft | | | |
| | | | | | Version 0.0.2 Editor's internal draft | | | |
| | | N1-001060 | | | Version 0.0.3 Submitted to CN1 SIP adhoc #1 | | | |
| 19/10/00 | | N1-001109 | | | Version 0.0.4 Reflecting results of initial CN1 discussion | | | |
| 19/10/00 | | N1-001115 | | | Version 0.0.5 Reflecting output of CN1 SIP adhoc#1 discussion | | | |
| 09/11/00 | | | | | Version 0.0.6 Revision to include latest template and styles | | | |
| | | N1-010092 | | | Version 0.0.7 Reflecting updates of some IETF drafts | | | |
| 14/02/01 | | N1-010269 | | | Version 0.0.8 Revision to include temporary annex B incorporating valuable source material | | | |
| 18/03/01 | | N1-010378 rev | | | Version 0.1.0 incorporating results of CN1 discussion at CN1 #16 | | | |
| 12/04/01 | | N1-010737 | | | Version 0.2.0 incorporating results of CN1 discussions at SIP adhoc #4 | | | |
| 11/06/01 | | N1-010935 | | | Version 0.3.0 incorporating results of CN1 discussions at CN1 #16 | | | |
| 23/07/01 | | N1-011103 | | | Version 0.4.0 incorporating results of CN1 discussions at CN1 #18 (agreed documents N1-011028, N1-011050, N1-011055, N1-011056) | | | |
| 12/09/01 | | N1-011385 | | | Version 0.5.0 incorporating results of CN1 discussions at CN1 #19 (agreed documents N1-011109, N1-011152, N1-011195, N1-011312, N1-011319, N1-011343) | | | |
| 04/10/01 | | N1-011470 | | | Version 0.6.0 incorporating results of CN1 discussions at CN1 #19bis (agreed documents N1-011346, N1-011373, N1-011389, N1-011390, N1-011392, N1-011393, N1-011394, N1-011408, N1-011410, N1-011426) | | | |
| 19/10/01 | | N1-011643 | | | Version 0.7.0 incorporating results of CN1 discussions at CN1 #20 (agreed documents N1-011477, N1-011479, N1-011498, N1-011523, N1-011548, N1-011585, N1-011586, N1-011592, N1-011611, N1-011629) | | | |
| 16/11/01 | | N1-011821 | | | Version 0.8.0 incorporating results of CN1 discussions at CN1 #20bis (agreed documents N1-011685, N1-011690, N1-011741, N1-011743, N1-011759, N1-011760, N1-011761, N1-011765c, N1-011767, N1-011769, N1-011770, N1-011771, N1-011774, N1-011777, N1-011779, N1-011780) N1-011712 was agreed but determined to have no impact on the specification at this time. | | | |
| 30/11/01 | | N1-020010 | | | Version 1.0.0 incorporating results of CN1 discussions at CN1 #21 (agreed documents N1-011828, N1-011829, N1-011836, N1-011899 [revision marks not used on moved text - additional change from chairman's report incorporated], implementation of subclause 3.1 editor's note based on discussion of N1-011900 [chairman's report], N1-011905, N1-011984, N1-011985, N1-011986, N1-011988, N1-011989, N1-012012 [excluding points 2 and 16], N1-012013, N1-012014 [excluding point 1], N1-012015, N1-012021, N1-012022, N1-012025, N1-012031, N1-012045, N1-012056, N1-012057) CN1 agreed for presentation for information to CN plenary. | | | |
| 18/01/02 | | N1-020189 | | | Version 1.1.0 incorporating results of CN1 discussions at CN1 SIP ad-hoc (agreed documents N1-020015, N1-020053, N1-020064, N1-020101, N1-020123, N1-020124, N1-020142, N1-020146, N1-020147, N1-020148, N1-020151, N1-020157, N1-020159, N1-020165). Also N1-012000 (agreed at previous meeting) required, subclause 5.2.6 to be deleted and this | | | |

| Change history | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Date** | **TSG #** | **TSG Doc.** | **CR** | **Rev** | **Subject/Comment** | **Old** | **New** | **WG doc** |
| | | | | | change has been enacted | | | |
| 01/02/02 | | N1-020459 | | | Version 1.2.0 incorporating results of CN1 discussions at CN1 #22 (agreed documents N1-020198, N1-020396, N1-020398, N1-020399, N1-020408, N1-020417, N1-020418, N1-020419, N1-020421, N1-020422, N1-020436, N1-020437, N1-020449) | | | |
| 01/02/02 | | N1-020569 | | | Version 1.2.1 issues to correct cut and paste error in incorporation of Annex B into main document. Affected subclause 5.1.1.3. Change to clause 7 title that was incorrectly applied to subclause 7.2 also corrected. | | | |
| 22/02/02 | | | | | Advanced to version 2.0.0 based on agreement of N1-020515.<br>Version 2.0.0 incorporating results of CN1 discussions at CN1 #22bis (agreed documents N1-020466, N1-020468, N1-020469, N1-020472, N1-020473, N1-020500, N1-020504, N1-020507, N1-020511, N1-020512, N1-020521, N1-020583, N1-020584, N1-020602, N1-020603, N1-020604, N1-020611, N1-020612, N1-020613, N1-020614, N1-020615, N1-020617, N1-020623, N1-020624, N1-020625, N1-020626, N1-020627, N1-020642, N1-020643, N1-020646, N1-020649, N1-020656, N1-020659, N1-020668, N1-020669, N1-020670, N1-020671).<br>In addition N1-020409, agreed at CN1#22 but missed from the previous version, was also implemented.<br>References have been resequenced. | | | |
| 02/03/02 | | | | | Editorial clean-up by ETSI/MCC. | 2.0.0 | 2.0.1 | |
| 11/03/02 | TSG CN#15 | NP-020049 | | | The draft was approved, and 3GPP TS 24.229 was then to be issued in Rel-5 under formal change control. | 2.0.1 | 5.0.0 | |
| 2002-06 | NP-16 | NP-020230 | 004 | 1 | S-CSCF Actions on Authentication Failure | 5.0.0 | 5.1.0 | N1-020903 |
| 2002-06 | NP-16 | NP-020230 | 005 | 2 | Disallow Parallel Registrations | 5.0.0 | 5.1.0 | N1-020959 |
| 2002-06 | NP-16 | NP-020230 | 007 | 1 | Hiding | 5.0.0 | 5.1.0 | N1-020910 |
| 2002-06 | NP-16 | NP-020312 | 008 | 8 | Support for services for unregistered users | 5.0.0 | 5.1.0 | |
| 2002-06 | | | 009 | 1 | Not implemented nor implementable. In the meeting report CN1#24 under doc N1-021513 it is shown that CR095r2 supercedes 009r1 if 095r2 was to be approved in CN#16 (but unfortunately 009r1 was also approved in the the CN#16 draft minutes). | | | N1-020921 |
| 2002-06 | NP-16 | NP-020231 | 019 | | MGCF procedure clarification | 5.0.0 | 5.1.0 | N1-020788 |
| 2002-06 | NP-16 | NP-020231 | 020 | 2 | MGCF procedure error cases | 5.0.0 | 5.1.0 | N1-020960 |
| 2002-06 | NP-16 | NP-020231 | 022 | 1 | Abbreviations clean up | 5.0.0 | 5.1.0 | N1-020949 |
| 2002-06 | NP-16 | NP-020231 | 023 | | Clarification of SIP usage outside IM CN subsystem | 5.0.0 | 5.1.0 | N1-020792 |
| 2002-06 | NP-16 | NP-020314 | 024 | 3 | Replacement of COMET by UPDATE | 5.0.0 | 5.1.0 | |
| 2002-06 | NP-16 | NP-020231 | 025 | 3 | Incorporation of current RFC numbers | 5.0.0 | 5.1.0 | N1-021091 |
| 2002-06 | NP-16 | NP-020231 | 026 | 1 | Clarification of B2BUA usage in roles | 5.0.0 | 5.1.0 | N1-020941 |
| 2002-06 | NP-16 | NP-020231 | 028 | 4 | Determination of MO / MT requests in I-CSCF(THIG) | 5.0.0 | 5.1.0 | N1-021248 |
| 2002-06 | NP-16 | NP-020231 | 030 | 2 | P-CSCF release of an existing session | 5.0.0 | 5.1.0 | N1-021006 |
| 2002-06 | NP-16 | NP-020232 | 031 | 1 | S-CSCF release of an existing session | 5.0.0 | 5.1.0 | N1-020939 |
| 2002-06 | NP-16 | NP-020232 | 033 | 3 | SDP procedure at the UE | 5.0.0 | 5.1.0 | N1-020971 |
| 2002-06 | NP-16 | NP-020232 | 035 | 1 | AS Procedures corrections | 5.0.0 | 5.1.0 | N1-020934 |
| 2002-06 | NP-16 | NP-020232 | 036 | 8 | Corrections to SIP Compression | 5.0.0 | 5.1.0 | N1-021499 |

| Change history | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Date** | **TSG #** | **TSG Doc.** | **CR** | **Rev** | **Subject/Comment** | **Old** | **New** | **WG doc** |
| 2002-06 | NP-16 | NP-020232 | 037 | 1 | Enhancement of S-CSCF and I-CSCF Routing Procedures for interworking with external networks | 5.0.0 | 5.1.0 | N1-020928 |
| 2002-06 | NP-16 | NP-020232 | 041 | 2 | Delivery of IMS security parameters from S-CSCF to the P-CSCF by using proprietary auth-param | 5.0.0 | 5.1.0 | N1-021003 |
| 2002-06 | NP-16 | NP-020232 | 045 | | Cleanup of request / response terminology - clause 5 | 5.0.0 | 5.1.0 | N1-020835 |
| 2002-06 | NP-16 | NP-020232 | 046 | | Cleanup of request / response terminology - clause 6 | 5.0.0 | 5.1.0 | N1-020836 |
| 2002-06 | NP-16 | NP-020232 | 047 | 2 | Simplification of profile tables | 5.0.0 | 5.1.0 | N1-021059 |
| 2002-06 | NP-16 | NP-020232 | 049 | | Forking options | 5.0.0 | 5.1.0 | N1-020839 |
| 2002-06 | NP-16 | NP-020315 | 050 | 1 | Media-Authorization header corrections | 5.0.0 | 5.1.0 | |
| 2002-06 | NP-16 | NP-020233 | 051 | 1 | Clause 5.4 editorials (S-CSCF) | 5.0.0 | 5.1.0 | N1-020950 |
| 2002-06 | NP-16 | NP-020233 | 053 | 2 | Integrity protection signalling from the P-CSCF to the S-CSCF | 5.0.0 | 5.1.0 | N1-021007 |
| 2002-06 | NP-16 | NP-020233 | 054 | | Representing IM CN subsystem functional entities in profile table roles | 5.0.0 | 5.1.0 | N1-020847 |
| 2002-06 | NP-16 | NP-020233 | 055 | | Clause 4 editorials | 5.0.0 | 5.1.0 | N1-020848 |
| 2002-06 | NP-16 | NP-020233 | 056 | | Clause 5.8 editorials (MRFC) | 5.0.0 | 5.1.0 | N1-020849 |
| 2002-06 | NP-16 | NP-020233 | 057 | 1 | Annex A editorials, including precondition additions | 5.0.0 | 5.1.0 | N1-021001 |
| 2002-06 | NP-16 | NP-020233 | 058 | 2 | Representing the registrar as a UA | 5.0.0 | 5.1.0 | N1-021054 |
| 2002-06 | NP-16 | NP-020233 | 059 | | Additional definitions | 5.0.0 | 5.1.0 | N1-020852 |
| 2002-06 | NP-16 | NP-020312 | 060 | 11 | Restructuring of S-CSCF Registration Sections | 5.0.0 | 5.1.0 | |
| 2002-06 | NP-16 | NP-020234 | 061 | 2 | Determination of MOC / MTC at P-CSCF and S-CSCF | 5.0.0 | 5.1.0 | N1-021060 |
| 2002-06 | NP-16 | NP-020234 | 062 | | Correction to the terminating procedures | 5.0.0 | 5.1.0 | N1-020927 |
| 2002-06 | NP-16 | NP-020234 | 063 | | Loose Routing for Network Initiated Call Release Procedures | 5.0.0 | 5.1.0 | N1-020940 |
| 2002-06 | NP-16 | NP-020234 | 064 | | Incorporation of previously agreed corrections to clause 5.2.5.2 (N1-020416) | 5.0.0 | 5.1.0 | N1-021004 |
| 2002-06 | NP-16 | NP-020234 | 065 | | Clause 7.2 editorial corrections | 5.0.0 | 5.1.0 | N1-021005 |
| 2002-06 | NP-16 | NP-020234 | 067 | 2 | S-CSCF routing of MO calls | 5.0.0 | 5.1.0 | N1-021097 |
| 2002-06 | NP-16 | NP-020234 | 068 | 1 | I-CSCF routeing of dialog requests | 5.0.0 | 5.1.0 | N1-021078 |
| 2002-06 | NP-16 | NP-020234 | 069 | 2 | Definition of the Tokanised-by parameter | 5.0.0 | 5.1.0 | N1-021096 |
| 2002-06 | NP-16 | NP-020235 | 070 | 3 | SDP procedures at UE | 5.0.0 | 5.1.0 | N1-021453 |
| 2002-06 | NP-16 | NP-020235 | 073 | 2 | Updates to the procedures involving the iFCs, following the Oulu iFC changes | 5.0.0 | 5.1.0 | N1-021440 |
| 2002-06 | NP-16 | NP-020235 | 074 | 1 | Addition of DHCPv6 references to 24.229 | 5.0.0 | 5.1.0 | N1-021086 |
| 2002-06 | NP-16 | NP-020235 | 075 | 1 | Clarification to URL and address assignments | 5.0.0 | 5.1.0 | N1-021083 |
| 2002-06 | NP-16 | NP-020235 | 079 | 3 | Downloading the implicitely registered public user identities from the S-CSCF to P-CSCF | 5.0.0 | 5.1.0 | N1-021510 |
| 2002-06 | NP-16 | NP-020235 | 080 | 3 | Clarification of GPRS aspects | 5.0.0 | 5.1.0 | N1-021486 |
| 2002-06 | NP-16 | NP-020235 | 081 | 2 | Introduction of Subscription Locator Function Interrogation at I-CSCF in 24.229 | 5.0.0 | 5.1.0 | N1-021469 |
| 2002-06 | NP-16 | NP-020235 | 082 | 1 | Introduction of Visited_Network_ID p-header | 5.0.0 | 5.1.0 | N1-021433 |
| 2002-06 | NP-16 | NP-020236 | 084 | 1 | MRFC register addresses | 5.0.0 | 5.1.0 | N1-021434 |
| 2002-06 | NP-16 | NP-020236 | 085 | 1 | MRFC INVITE interface editor's notes | 5.0.0 | 5.1.0 | N1-021470 |
| 2002-06 | NP-16 | NP-020236 | 086 | 1 | MRFC OPTIONS interface editor's notes | 5.0.0 | 5.1.0 | N1-021471 |
| 2002-06 | NP-16 | NP-020236 | 087 | | MRFC PRACK & INFO editor's notes | 5.0.0 | 5.1.0 | N1-021159 |

| Change history | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Date | TSG # | TSG Doc. | CR | Rev | Subject/Comment | Old | New | WG doc |
| 2002-06 | NP-16 | NP-020236 | 088 | 1 | MGCF OPTIONS interface editor's notes | 5.0.0 | 5.1.0 | N1-021472 |
| 2002-06 | NP-16 | NP-020236 | 089 | | MGCF reINVITE editor's notes | 5.0.0 | 5.1.0 | N1-021161 |
| 2002-06 | NP-16 | NP-020237 | 090 | | 3PCC AS editor's notes | 5.0.0 | 5.1.0 | N1-021162 |
| 2002-06 | NP-16 | NP-020237 | 091 | | AS acting as terminating UA editor's notes | 5.0.0 | 5.1.0 | N1-021163 |
| 2002-06 | NP-16 | NP-020237 | 092 | 1 | AS acting as originating UA editor's notes | 5.0.0 | 5.1.0 | N1-021466 |
| 2002-06 | NP-16 | NP-020237 | 093 | 2 | Charging overview clause | 5.0.0 | 5.1.0 | N1-021512 |
| 2002-06 | NP-16 | NP-020237 | 094 | 1 | Procedures for original-dialog-id P-header | 5.0.0 | 5.1.0 | N1-021456 |
| 2002-06 | NP-16 | NP-020237 | 095 | 2 | Procedures for charging-vector P-header | 5.0.0 | 5.1.0 | N1-021513 |
| 2002-06 | NP-16 | NP-020237 | 096 | 1 | Procedures for charging-function-addresses P-header | 5.0.0 | 5.1.0 | N1-021458 |
| 2002-06 | NP-16 | NP-020237 | 097 | 1 | SDP types | 5.0.0 | 5.1.0 | N1-021467 |
| 2002-06 | NP-16 | NP-020237 | 100 | | Removal of State from profile tables | 5.0.0 | 5.1.0 | N1-021173 |
| 2002-06 | NP-16 | NP-020238 | 101 | | Editor's note cleanup - clause 3 | 5.0.0 | 5.1.0 | N1-021174 |
| 2002-06 | NP-16 | NP-020238 | 102 | | Editor's note cleanup - clause 4 | 5.0.0 | 5.1.0 | N1-021175 |
| 2002-06 | NP-16 | NP-020238 | 103 | | Editor's note cleanup - clause 5.1 and deletion of void subclauses | 5.0.0 | 5.1.0 | N1-021176 |
| 2002-06 | NP-16 | NP-020238 | 104 | 1 | Editor's note cleanup - clause 5.2 and deletion of void subclauses | 5.0.0 | 5.1.0 | N1-021487 |
| 2002-06 | NP-16 | NP-020238 | 105 | | Editor's note cleanup - clause 5.3 | 5.0.0 | 5.1.0 | N1-021178 |
| 2002-06 | NP-16 | NP-020238 | 106 | | Editor's note cleanup - clause 5.4 and deletion of void subclauses | 5.0.0 | 5.1.0 | N1-021179 |
| 2002-06 | NP-16 | NP-020238 | 107 | | Editor's note cleanup - clause 5.5 and deletion of void subclauses | 5.0.0 | 5.1.0 | N1-021180 |
| 2002-06 | NP-16 | NP-020238 | 110 | | Editor's note cleanup - clause 6 | 5.0.0 | 5.1.0 | N1-021183 |
| 2002-06 | NP-16 | NP-020238 | 111 | | Editor's note cleanup - clause 9 | 5.0.0 | 5.1.0 | N1-021184 |
| 2002-06 | NP-16 | NP-020239 | 113 | 1 | SIP Default Timers | 5.0.0 | 5.1.0 | N1-021465 |
| 2002-06 | NP-16 | NP-020239 | 114 | 1 | Correction of the subscription to the registration event package | 5.0.0 | 5.1.0 | N1-021436 |
| 2002-06 | NP-16 | NP-020239 | 115 | 1 | Support for ISIMless UICC | 5.0.0 | 5.1.0 | N1-021441 |
| 2002-06 | NP-16 | NP-020239 | 119 | 1 | SIP procedures at UE | 5.0.0 | 5.1.0 | N1-021452 |
| 2002-06 | NP-16 | NP-020239 | 121 | 2 | New requirements in the P-CSCF | 5.0.0 | 5.1.0 | N1-021509 |
| 2002-06 | NP-16 | NP-020239 | 122 | | SDP procedures at MGCF | 5.0.0 | 5.1.0 | N1-021264 |
| 2002-06 | NP-16 | NP-020239 | 124 | 1 | S-CSCF allocation | 5.0.0 | 5.1.0 | N1-021443 |
| 2002-06 | NP-16 | NP-020240 | 129 | 1 | Introduction of P-Access-Network-Info header | 5.0.0 | 5.1.0 | N1-021498 |
| 2002-06 | NP-16 | NP-020240 | 130 | 2 | Usage of Path and P-Service Route | 5.0.0 | 5.1.0 | N1-021508 |
| 2002-06 | NP-16 | NP-020240 | 133 | | Removal of Referred-By header from specification | 5.0.0 | 5.1.0 | N1-021354 |
| 2002-06 | NP-16 | NP-020240 | 134 | | Handling of Record-Route header in profile tables | 5.0.0 | 5.1.0 | N1-021357 |
| 2002-06 | NP-16 | NP-020312 | 135 | 1 | Asserted identities and privacy | 5.0.0 | 5.1.0 | |
| 2002-06 | NP-16 | NP-020240 | 136 | | Removal of caller preferences from specification | 5.0.0 | 5.1.0 | N1-021359 |
| 2002-06 | NP-16 | NP-020240 | 137 | | Substitution of REFER references | 5.0.0 | 5.1.0 | N1-021360 |
| 2002-06 | NP-16 | NP-020240 | 138 | | Removal of session timer from specification | 5.0.0 | 5.1.0 | N1-021361 |
| 2002-09 | NP-17 | NP-020489 | 141 | 2 | Adding MESSAGE to 24.229 | 5.1.0 | 5.2.0 | |

| Change history | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Date | TSG # | TSG Doc. | CR | Rev | Subject/Comment | Old | New | WG doc |
| 2002-09 | NP-17 | NP-020375 | 142 | | Public user identity to use for third party register | 5.1.0 | 5.2.0 | N1-021563 |
| 2002-09 | NP-17 | NP-020375 | 143 | 1 | Replace P-Original-Dialog-ID header with unique data in Route header | 5.1.0 | 5.2.0 | N1-021797 |
| 2002-09 | NP-17 | NP-020375 | 145 | | Synchronize text with latest I-D for P-headers for charging | 5.1.0 | 5.2.0 | N1-021569 |
| 2002-09 | NP-17 | NP-020488 | 146 | 2 | Service profiles and implicitly registered public user identities | 5.1.0 | 5.2.0 | |
| 2002-09 | NP-17 | NP-020376 | 147 | | S-CSCF decides when to include IOI | 5.1.0 | 5.2.0 | N1-021571 |
| 2002-09 | NP-17 | NP-020376 | 148 | | Clean up XML in clause 7.6 | 5.1.0 | 5.2.0 | N1-021572 |
| 2002-09 | NP-17 | NP-020376 | 149 | | Fix clause 5.2.7.4 header | 5.1.0 | 5.2.0 | N1-021573 |
| 2002-09 | NP-17 | NP-020376 | 150 | | Removal of forward reference to non P-CSCF procedures | 5.1.0 | 5.2.0 | N1-021589 |
| 2002-09 | NP-17 | NP-020376 | 151 | | Deregistration of public user identities | 5.1.0 | 5.2.0 | N1-021590 |
| 2002-09 | NP-17 | NP-020376 | 152 | | Reauthentication trigger via other means | 5.1.0 | 5.2.0 | N1-021591 |
| 2002-09 | NP-17 | NP-020487 | 153 | 3 | Registration with integrity protection | 5.1.0 | 5.2.0 | |
| 2002-09 | NP-17 | NP-020485 | 154 | 2 | Explicit listing of need to route response messages | 5.1.0 | 5.2.0 | |
| 2002-09 | NP-17 | NP-020377 | 157 | 1 | Include IP address in ICID | 5.1.0 | 5.2.0 | N1-021816 |
| 2002-09 | NP-17 | NP-020377 | 158 | | Reference updates | 5.1.0 | 5.2.0 | N1-021604 |
| 2002-09 | NP-17 | NP-020377 | 159 | | Abbreviation updates | 5.1.0 | 5.2.0 | N1-021605 |
| 2002-09 | NP-17 | NP-020377 | 163 | 1 | Clarifications of allocation of IP address | 5.1.0 | 5.2.0 | N1-021817 |
| 2002-09 | NP-17 | NP-020377 | 171 | 1 | Verifications at the P-CSCF for subsequent request | 5.1.0 | 5.2.0 | N1-021802 |
| 2002-09 | NP-17 | NP-020377 | 174 | 1 | Clarification of IMS signalling flag | 5.1.0 | 5.2.0 | N1-021781 |
| 2002-09 | NP-17 | NP-020377 | 176 | 1 | Definition of a general-purpose PDP context for IMS | 5.1.0 | 5.2.0 | N1-021783 |
| 2002-09 | NP-17 | NP-020372 | 177 | 2 | Request for DNS IPv6 server address | 5.1.0 | 5.2.0 | N1-021833 |
| 2002-09 | NP-17 | NP-020378 | 178 | | Error cases for PDP context modification | 5.1.0 | 5.2.0 | N1-021679 |
| 2002-09 | NP-17 | NP-020378 | 183 | 1 | Incorporation of draft-ietf-sip-sec-agree-04.txt | 5.1.0 | 5.2.0 | N1-021791 |
| 2002-09 | NP-17 | NP-020378 | 185 | 1 | User Initiated De-registration | 5.1.0 | 5.2.0 | N1-021787 |
| 2002-09 | NP-17 | NP-020378 | 186 | 1 | Mobile initiated de-registration | 5.1.0 | 5.2.0 | N1-021788 |
| 2002-09 | NP-17 | NP-020378 | 187 | 1 | CallID of REGISTER requests | 5.1.0 | 5.2.0 | N1-021786 |
| 2002-09 | NP-17 | NP-020378 | 188 | 1 | Correction to the I-CSCF routing procedures | 5.1.0 | 5.2.0 | N1-021803 |
| 2002-09 | NP-17 | NP-020378 | 189 | 1 | Registration procedures at P-CSCF | 5.1.0 | 5.2.0 | N1-021793 |
| 2002-09 | NP-17 | NP-020378 | 192 | 1 | Corrections related to the P-Access-Network-Info header | 5.1.0 | 5.2.0 | N1-021827 |
| 2002-09 | NP-17 | NP-020378 | 194 | 1 | Chapter to decribe the registration event | 5.1.0 | 5.2.0 | N1-021794 |
| 2002-09 | NP-17 | NP-020484 | 196 | | Definition of abbreviation IMS | 5.1.0 | 5.2.0 | |
| 2002-12 | NP-18 | NP-020558 | 140 | 4 | Support of non-IMS forking | 5.2.0 | 5.3.0 | N1-022446 |
| 2002-12 | NP-18 | NP-020565 | 144 | 2 | Identification of supported IETF drafts within this release | 5.2.0 | 5.3.0 | N1-022114 |
| 2002-12 | NP-18 | NP-020558 | 161 | 3 | Clarifications and editorials to SIP profile | 5.2.0 | 5.3.0 | N1-022412 |
| 2002-12 | NP-18 | NP-020558 | 175 | 5 | Clarifications of the binding and media grouping | 5.2.0 | 5.3.0 | N1-022494 |
| 2002-12 | NP-18 | NP-020558 | 179 | 2 | Support of originating requests from Application Servers | 5.2.0 | 5.3.0 | N1-022106 |

| Change history | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Date** | **TSG #** | **TSG Doc.** | **CR** | **Rev** | **Subject/Comment** | **Old** | **New** | **WG doc** |
| 2002-12 | NP-18 | NP-020558 | 197 | | Wrong references in 4.1 | 5.2.0 | 5.3.0 | N1-021902 |
| 2002-12 | NP-18 | NP-020558 | 198 | | Alignment of the MGCF procedures to RFC 3312 | 5.2.0 | 5.3.0 | N1-021903 |
| 2002-12 | NP-18 | NP-020558 | 199 | 1 | Service Route Header and Path Header interactions | 5.2.0 | 5.3.0 | N1-022080 |
| 2002-12 | NP-18 | NP-020558 | 202 | | Addition of clause 6 though clause 9 references to conformance clause | 5.2.0 | 5.3.0 | N1-021919 |
| 2002-12 | NP-18 | NP-020558 | 203 | 1 | URL and address assignments | 5.2.0 | 5.3.0 | N1-022115 |
| 2002-12 | NP-18 | NP-020559 | 204 | 3 | Fix gprs-charging-info definition and descriptions | 5.2.0 | 5.3.0 | N1-022426 |
| 2002-12 | NP-18 | NP-020559 | 206 | | Alignment of the SDP attributes related to QoS integration with IETF | 5.2.0 | 5.3.0 | N1-021930 |
| 2002-12 | NP-18 | NP-020559 | 207 | 1 | Update of the 3GPP-generated SIP P- headers document references | 5.2.0 | 5.3.0 | N1-022116 |
| 2002-12 | NP-18 | NP-020559 | 208 | 1 | Handling of INVITE requests that do not contain SDP | 5.2.0 | 5.3.0 | N1-022098 |
| 2002-12 | NP-18 | NP-020559 | 209 | 2 | UE Registration | 5.2.0 | 5.3.0 | N1-022471 |
| 2002-12 | NP-18 | NP-020559 | 211 | 1 | Usage of private user identity during registration | 5.2.0 | 5.3.0 | N1-022083 |
| 2002-12 | NP-18 | NP-020559 | 212 | 1 | P-CSCF subscription to the users registration-state event | 5.2.0 | 5.3.0 | N1-022084 |
| 2002-12 | NP-18 | NP-020559 | 213 | 2 | Handling of MT call by the P-CSCF | 5.2.0 | 5.3.0 | N1-022154 |
| 2002-12 | NP-18 | NP-020559 | 215 | | P-CSCF acting as a UA | 5.2.0 | 5.3.0 | N1-021939 |
| 2002-12 | NP-18 | NP-020559 | 216 | 1 | S-CSCF handling of protected registrations | 5.2.0 | 5.3.0 | N1-022085 |
| 2002-12 | NP-18 | NP-020560 | 217 | 1 | S-CSCF handling of subscription to the users registration-state event | 5.2.0 | 5.3.0 | N1-022086 |
| 2002-12 | NP-18 | NP-020560 | 218 | 1 | Determination of MO or MT in I-CSCF | 5.2.0 | 5.3.0 | N1-022102 |
| 2002-12 | NP-18 | NP-020560 | 220 | | Definition of the NAI and RTCP abbreviations | 5.2.0 | 5.3.0 | N1-021944 |
| 2002-12 | NP-18 | NP-020560 | 222 | 4 | Go related error codes in the UE | 5.2.0 | 5.3.0 | N1-022495 |
| 2002-12 | NP-18 | NP-020560 | 223 | 1 | Clarifications on CCF/ECF addresses | 5.2.0 | 5.3.0 | N1-022120 |
| 2002-12 | NP-18 | NP-020560 | 225 | 2 | Clarifications on dedicated PDP Context for IMS signaling | 5.2.0 | 5.3.0 | N1-022156 |
| 2002-12 | NP-18 | NP-020560 | 228 | 3 | Clarifications on the use of charging correlation information | 5.2.0 | 5.3.0 | N1-022425 |
| 2002-12 | NP-18 | NP-020560 | 232 | 1 | Expires information in REGISTER response | 5.2.0 | 5.3.0 | N1-022095 |
| 2002-12 | NP-18 | NP-020560 | 235 | 2 | Indication of successful establishment of Dedicated Signalling PDP context to the UE | 5.2.0 | 5.3.0 | N1-022129 |
| 2002-12 | NP-18 | NP-020560 | 237 | | P-CSCF sending 100 (Trying) Response for reINVITE | 5.2.0 | 5.3.0 | N1-021998 |
| 2002-12 | NP-18 | NP-020561 | 239 | 1 | Correction on P-Asserted-Id, P-Preferred-Id, Remote-Party-ID | 5.2.0 | 5.3.0 | N1-022100 |
| 2002-12 | NP-18 | NP-020561 | 240 | 1 | Clarifications to subclause 9.2.5 | 5.2.0 | 5.3.0 | N1-022137 |
| 2002-12 | NP-18 | NP-020561 | 242 | | ENUM translation | 5.2.0 | 5.3.0 | N1-022020 |
| 2002-12 | NP-18 | NP-020561 | 243 | 1 | AS routing | 5.2.0 | 5.3.0 | N1-022107 |
| 2002-12 | NP-18 | NP-020561 | 245 | 1 | Warning header | 5.2.0 | 5.3.0 | N1-022108 |
| 2002-12 | NP-18 | NP-020561 | 246 | 3 | S-CSCF procedure tidyup | 5.2.0 | 5.3.0 | N1-022497 |

| Change history | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Date** | **TSG #** | **TSG Doc.** | **CR** | **Rev** | **Subject/Comment** | **Old** | **New** | **WG doc** |
| 2002-12 | NP-18 | NP-020561 | 247 | 1 | P-CSCF procedure tidyup | 5.2.0 | 5.3.0 | N1-022125 |
| 2002-12 | NP-18 | NP-020561 | 248 | 2 | UE procedure tidyup | 5.2.0 | 5.3.0 | N1-022472 |
| 2002-12 | NP-18 | NP-020561 | 249 | 3 | MESSAGE corrections part 1 | 5.2.0 | 5.3.0 | N1-022455 |
| 2002-12 | NP-18 | NP-020561 | 250 | 2 | MESSAGE corrections part 2 | 5.2.0 | 5.3.0 | N1-022456 |
| 2002-12 | NP-18 | NP-020562 | 251 | 2 | Security association clarifications | 5.2.0 | 5.3.0 | N1-022440 |
| 2002-12 | NP-18 | NP-020562 | 252 | 1 | The use of security association by the UE | 5.2.0 | 5.3.0 | N1-022433 |
| 2002-12 | NP-18 | NP-020562 | 253 | 1 | UE integrity protected re-registration | 5.2.0 | 5.3.0 | N1-022434 |
| 2002-12 | NP-18 | NP-020562 | 255 | 3 | Handling of default public user identities by the P-CSCF | 5.2.0 | 5.3.0 | N1-022496 |
| 2002-12 | NP-18 | NP-020562 | 263 | | Fixing ioi descriptions | 5.2.0 | 5.3.0 | N1-022266 |
| 2002-12 | NP-18 | NP-020562 | 264 | 1 | Fix descriptions for ECF/CCF addresses | 5.2.0 | 5.3.0 | N1-022447 |
| 2002-12 | NP-18 | NP-020562 | 266 | 2 | Alignment with draft-ietf-sipping-reg-event-00 and clarification on network initiated deregistration | 5.2.0 | 5.3.0 | N1-022493 |
| 2002-12 | NP-18 | NP-020563 | 267 | 1 | Correction to network initiated re-authentication procedure | 5.2.0 | 5.3.0 | N1-022449 |
| 2002-12 | NP-18 | NP-020563 | 268 | 1 | Registration Expires Timer Default Setting | 5.2.0 | 5.3.0 | N1-022439 |
| 2002-12 | NP-18 | NP-020563 | 269 | 1 | Clarification on Sh interface for charging purposes | 5.2.0 | 5.3.0 | N1-022465 |
| 2002-12 | NP-18 | NP-020563 | 270 | 2 | Clarifications on the scope | 5.2.0 | 5.3.0 | N1-022500 |
| 2002-12 | NP-18 | NP-020563 | 273 | 1 | Add charging info for SUBSCRIBE | 5.2.0 | 5.3.0 | N1-022467 |
| 2002-12 | NP-18 | NP-020563 | 274 | 1 | Profile revisions for RFC 3261 headers | 5.2.0 | 5.3.0 | N1-022413 |
| 2002-12 | NP-18 | NP-020563 | 275 | | Consistency changes for SDP procedures at MGCF | 5.2.0 | 5.3.0 | N1-022345 |
| 2002-12 | NP-18 | NP-020563 | 276 | | Proxy support of PRACK | 5.2.0 | 5.3.0 | N1-022350 |
| 2002-12 | NP-18 | NP-020563 | 277 | | Clarification of transparent handling of parameters in profile | 5.2.0 | 5.3.0 | N1-022351 |
| 2002-12 | NP-18 | NP-020564 | 279 | 1 | Meaning of refresh request | 5.2.0 | 5.3.0 | N1-022444 |
| 2002-12 | NP-18 | NP-020564 | 280 | | Removal of Caller Preferences dependency | 5.2.0 | 5.3.0 | N1-022362 |
| 2002-12 | NP-18 | NP-020564 | 281 | 1 | P-Access-Network-Info clarifications | 5.2.0 | 5.3.0 | N1-022445 |
| 2002-12 | NP-18 | NP-020564 | 282 | | Clarification on use of the From header by the UE | 5.2.0 | 5.3.0 | N1-022370 |
| 2002-12 | NP-18 | NP-020634 | 283 | 2 | Support of comp=sigcomp parameter | 5.2.0 | 5.3.0 | |
| 2002-12 | NP-18 | NP-020668 | 284 | 4 | SDP media policy rejection | 5.2.0 | 5.3.0 | |
| 2002-12 | NP-18 | NP-020567 | 285 | 1 | Fallback for compression failure | 5.2.0 | 5.3.0 | N1-022481 |
| 2002-12 | NP-18 | NP-020564 | 287 | 1 | SA related procedures | 5.2.0 | 5.3.0 | N1-022459 |
| 2002-12 | NP-18 | NP-020568 | 290 | 1 | Emergency Service correction | 5.2.0 | 5.3.0 | N1-022461 |
| 2002-12 | NP-18 | NP-020663 | 278 | 4 | P-CSCF does not strip away headers | 5.2.0 | 5.3.0 | N1-022499 |
| 2002-12 | NP-18 | NP-020557 | 289 | | PCF to PDF | 5.2.0 | 5.3.0 | N1-022387 |
| 2003-03 | NP-19 | NP-030049 | 291 | | Minor correction and consistency changes to general part of profile | 5.3.0 | 5.4.0 | N1-030012 |
| 2003-03 | NP-19 | NP-030049 | 292 | | SIP profile minor correction and consistency changes | 5.3.0 | 5.4.0 | N1-030013 |
| 2003-03 | NP-19 | NP-030049 | 293 | 1 | Network asserted identity procedure corrections for | 5.3.0 | 5.4.0 | N1-030261 |

| Change history | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Date | TSG # | TSG Doc. | CR | Rev | Subject/Comment | Old | New | WG doc |
| | | | | | the UE | | | |

| Change history | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Date** | **TSG #** | **TSG Doc.** | **CR** | **Rev** | **Subject/Comment** | **Old** | **New** | **WG doc** |
| 2003-03 | NP-19 | NP-030049 | 294 | 1 | Asserted identity inclusion in SIP profile | 5.3.0 | 5.4.0 | N1-030300 |
| 2003-03 | NP-19 | NP-030049 | 296 | | Profile references relating to registration | 5.3.0 | 5.4.0 | N1-030023 |
| 2003-03 | NP-19 | NP-030049 | 297 | 2 | Reference corrections | 5.3.0 | 5.4.0 | N1-030301 |
| 2003-03 | NP-19 | NP-030050 | 300 | 1 | 488 message with a subset of allowed media parameters | 5.3.0 | 5.4.0 | N1-030245 |
| 2003-03 | NP-19 | NP-030050 | 301 | 1 | Handling of Emergency Numbers in P-CSCF | 5.3.0 | 5.4.0 | N1-030239 |
| 2003-03 | NP-19 | NP-030050 | 302 | 2 | Correction of the registration state event package | 5.3.0 | 5.4.0 | N1-030268 |
| 2003-03 | NP-19 | NP-030050 | 305 | 2 | User initiated de-registration at P-CSCF | 5.3.0 | 5.4.0 | N1-030295 |
| 2003-03 | NP-19 | NP-030050 | 306 | 2 | Network-initiated deregistration at UE, P-CSCF, and S-CSCF | 5.3.0 | 5.4.0 | N1-030296 |
| 2003-03 | NP-19 | NP-030050 | 307 | 2 | UE deregistration during established dialogs | 5.3.0 | 5.4.0 | N1-030297 |
| 2003-03 | NP-19 | NP-030050 | 308 | 2 | S-CSCF handling of deregistration during established dialogs | 5.3.0 | 5.4.0 | N1-030298 |
| 2003-03 | NP-19 | NP-030050 | 309 | 1 | S-CSCF handling of established dialogs upon deregistration | 5.3.0 | 5.4.0 | N1-030233 |
| 2003-03 | NP-19 | NP-030050 | 310 | 2 | S-CSCF handling of established dialogs upon registration-lifetime expiration | 5.3.0 | 5.4.0 | N1-030299 |
| 2003-03 | NP-19 | NP-030051 | 311 | 1 | P-CSCF handling of established dialogs upon registration-lifetime expiration | 5.3.0 | 5.4.0 | N1-030235 |
| 2003-03 | NP-19 | NP-030051 | 312 | 1 | Correction of Authentication procedure | 5.3.0 | 5.4.0 | N1-030240 |
| 2003-03 | NP-19 | NP-030051 | 313 | | Mixed Path header and Service-Route operation | 5.3.0 | 5.4.0 | N1-030127 |
| 2003-03 | NP-19 | NP-030051 | 315 | 2 | Clarifications on updating the authorization token | 5.3.0 | 5.4.0 | N1-030255 |
| 2003-03 | NP-19 | NP-030051 | 318 | 2 | Consideration of P-CSCF/PDF | 5.3.0 | 5.4.0 | N1-030307 |
| 2003-03 | NP-19 | NP-030051 | 319 | 2 | Clarification on GPRS charging information | 5.3.0 | 5.4.0 | N1-030308 |
| 2003-03 | NP-19 | NP-030051 | 323 | 1 | P-Access-Network-Info procedure corrections for the UE | 5.3.0 | 5.4.0 | N1-030250 |
| 2003-03 | NP-19 | NP-030051 | 324 | 1 | P-Access-Network-Info procedure corrections for the S-CSCF | 5.3.0 | 5.4.0 | N1-030251 |
| 2003-03 | NP-19 | NP-030051 | 326 | 1 | Updating user agent related profile tables | 5.3.0 | 5.4.0 | N1-030260 |
| 2003-03 | NP-19 | NP-030052 | 327 | 2 | Cleanup and clarification to the registration and authentication procedure | 5.3.0 | 5.4.0 | N1-030282 |
| 2003-03 | NP-19 | NP-030052 | 328 | 1 | Corrections to the reg event package | 5.3.0 | 5.4.0 | N1-030230 |
| 2003-03 | NP-19 | NP-030052 | 330 | 2 | Clarifications for setting up separate PDP contexts in case of SBLP | 5.3.0 | 5.4.0 | N1-030288 |
| 2003-03 | NP-19 | NP-030052 | 331 | 2 | Handling of the P-Media-Autohorization header | 5.3.0 | 5.4.0 | N1-030289 |
| 2003-03 | NP-19 | NP-030052 | 333 | 3 | Removal of P-Asserted-Identity from clause 7 of 24.229 | 5.3.0 | 5.4.0 | N1-030310 |
| 2003-03 | NP-19 | NP-030052 | 334 | | P-CSCF general procedure corrections | 5.3.0 | 5.4.0 | N1-030182 |
| 2003-03 | NP-19 | NP-030052 | 335 | 2 | Usage of Contact in UE's registration procedure | 5.3.0 | 5.4.0 | N1-030281 |
| 2003-03 | NP-19 | NP-030052 | 337 | | Usage of P-Asserted-Identity for responses | 5.3.0 | 5.4.0 | N1-030193 |
| 2003-03 | NP-19 | NP-030052 | 339 | 2 | Authorization for registration event package | 5.3.0 | 5.4.0 | N1-030285 |
| 2003-03 | NP-19 | NP-030052 | 341 | 1 | P-CSCF subscription to reg event | 5.3.0 | 5.4.0 | N1-030284 |

| Change history | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Date** | **TSG #** | **TSG Doc.** | **CR** | **Rev** | **Subject/Comment** | **Old** | **New** | **WG doc** |
| 2003-06 | NP-20 | NP-030275 | 295 | 4 | Security agreement inclusion in SIP profile | 5.4.0 | 5.5.0 | N1-030939 |
| 2003-06 | NP-20 | NP-030275 | 322 | 5 | 3GPP P-header inclusion in SIP profile | 5.4.0 | 5.5.0 | N1-030938 |
| 2003-06 | NP-20 | NP-030275 | 332 | 5 | Change of IP address for the UE | 5.4.0 | 5.5.0 | N1-030923 |
| 2003-06 | NP-20 | NP-030275 | 342 | | Removal of the requirement for UE re-authentication initiated by HSS | 5.4.0 | 5.5.0 | N1-030349 |
| 2003-06 | NP-20 | NP-030275 | 343 | 2 | UE behaviour on reception of 420 (Bad Extension) message | 5.4.0 | 5.5.0 | N1-030552 |
| 2003-06 | NP-20 | NP-030275 | 347 | 2 | Handling of DTMF | 5.4.0 | 5.5.0 | N1-030551 |
| 2003-06 | NP-20 | NP-030276 | 348 | 1 | Format of Tel URL in P-Asserted-Id | 5.4.0 | 5.5.0 | N1-030510 |
| 2003-06 | NP-20 | NP-030276 | 349 | | Delete Note on header stripping/SDP manipulation | 5.4.0 | 5.5.0 | N1-030387 |
| 2003-06 | NP-20 | NP-030276 | 354 | 1 | Clarifications on using DNS procedures | 5.4.0 | 5.5.0 | N1-030520 |
| 2003-06 | NP-20 | NP-030276 | 356 | 4 | Addition of procedures at the AS for SDP | 5.4.0 | 5.5.0 | N1-030942 |
| 2003-06 | NP-20 | NP-030276 | 357 | 1 | Usage of P-Associated-URI | 5.4.0 | 5.5.0 | N1-030499 |
| 2003-06 | NP-20 | NP-030276 | 359 | 1 | Network-initiated deregistration at UE and P-CSCF | 5.4.0 | 5.5.0 | N1-030501 |
| 2003-06 | NP-20 | NP-030276 | 360 | 2 | Barred identities | 5.4.0 | 5.5.0 | N1-030550 |
| 2003-06 | NP-20 | NP-030276 | 365 | 1 | PDP contex subject to SBLP cannot be reused by other IMS sessions | 5.4.0 | 5.5.0 | N1-030513 |
| 2003-06 | NP-20 | NP-030276 | 368 | 1 | User authentication failure cleanups | 5.4.0 | 5.5.0 | N1-030506 |
| 2003-06 | NP-20 | NP-030277 | 369 | 3 | S-CSCF behavior correction to enable call forwarding | 5.4.0 | 5.5.0 | N1-030931 |
| 2003-06 | NP-20 | NP-030277 | 370 | 1 | SUBSCRIBE request information stored at the P-CSCF and S-CSCF | 5.4.0 | 5.5.0 | N1-030521 |
| 2003-06 | NP-20 | NP-030277 | 371 | 1 | Profile Tables - Transparency | 5.4.0 | 5.5.0 | N1-030858 |
| 2003-06 | NP-20 | NP-030277 | 375 | 1 | Profile Tables - Major Capability Corrections | 5.4.0 | 5.5.0 | N1-030860 |
| 2003-06 | NP-20 | NP-030277 | 376 | 2 | Profile Tables - Deletion of Elements not used in 24.229 | 5.4.0 | 5.5.0 | N1-030921 |
| 2003-06 | NP-20 | NP-030277 | 377 | 1 | Use of the QoS parameter 'signalling information' for a signalling PDP context | 5.4.0 | 5.5.0 | N1-030840 |
| 2003-06 | NP-20 | NP-030277 | 378 | 2 | Deregistration of a PUID (not the last one) | 5.4.0 | 5.5.0 | N1-030919 |
| 2003-06 | NP-20 | NP-030277 | 379 | 2 | 'Last registered public user identity' terminology change | 5.4.0 | 5.5.0 | N1-030920 |
| 2003-06 | NP-20 | NP-030277 | 380 | 1 | Check Integrity Protection for P-Access-Network-Info header | 5.4.0 | 5.5.0 | N1-030881 |
| 2003-06 | NP-20 | NP-030278 | 381 | 1 | PCSCF setting of Integrity protection indicator and checking of Security Verify header | 5.4.0 | 5.5.0 | N1-030882 |
| 2003-06 | NP-20 | NP-030278 | 383 | 1 | Consistent treatment of register and de-register | 5.4.0 | 5.5.0 | N1-030884 |
| 2003-06 | NP-20 | NP-030278 | 384 | 1 | Optionality of sending CK is removed | 5.4.0 | 5.5.0 | N1-030885 |
| 2003-06 | NP-20 | NP-030278 | 385 | 1 | Addition of note and Correction of References regarding security associations and registration | 5.4.0 | 5.5.0 | N1-030886 |
| 2003-06 | NP-20 | NP-030278 | 387 | 1 | Subscription/Registration refresh time | 5.4.0 | 5.5.0 | N1-030887 |
| 2003-06 | NP-20 | NP-030278 | 388 | 1 | Corrections to use of IK | 5.4.0 | 5.5.0 | N1-030863 |
| 2003-06 | NP-20 | NP-030278 | 390 | | Mobile-originating case at UE | 5.4.0 | 5.5.0 | N1-030647 |

| Change history | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Date | TSG # | TSG Doc. | CR | Rev | Subject/Comment | Old | New | WG doc |
| 2003-06 | NP-20 | NP-030278 | 394 | 2 | Re-authentication procedure. | 5.4.0 | 5.5.0 | N1-030917 |
| 2003-06 | NP-20 | NP-030278 | 395 | | Replacement of SIP URL with SIP URI | 5.4.0 | 5.5.0 | N1-030652 |
| 2003-06 | NP-20 | NP-030279 | 397 | 2 | Notification about registration state | 5.4.0 | 5.5.0 | N1-030926 |
| 2003-06 | NP-20 | NP-030279 | 402 | 1 | Handling of P-Asserted ID in MGCF | 5.4.0 | 5.5.0 | N1-030848 |
| 2003-06 | NP-20 | NP-030279 | 404 | 1 | S-CSCF initiated release of calls to circiut switched network | 5.4.0 | 5.5.0 | N1-030873 |
| 2003-06 | NP-20 | NP-030279 | 405 | 2 | Supported Integrity algorithms | 5.4.0 | 5.5.0 | N1-030927 |
| 2003-06 | NP-20 | NP-030279 | 407 | 1 | RFC 3524, Single Reservation Flows | 5.4.0 | 5.5.0 | N1-030851 |
| 2003-06 | NP-20 | NP-030279 | 410 | 1 | Clarification of the S-CSCF's handling of the P-access-network-info header | 5.4.0 | 5.5.0 | N1-030868 |
| 2003-06 | NP-20 | NP-030279 | 411 | 2 | Port numbers in the RR header entries | 5.4.0 | 5.5.0 | N1-030941 |
| 2003-06 | NP-20 | NP-030279 | 412 | 2 | Registration abnormal cases | 5.4.0 | 5.5.0 | N1-030928 |
| 2003-06 | NP-20 | NP-030280 | 415 | | Minor correction to section 5.4.5.1.2 | 5.4.0 | 5.5.0 | N1-030720 |
| 2003-06 | NP-20 | NP-030280 | 417 | 1 | Introduction of RTCP bandwidth | 5.4.0 | 5.5.0 | N1-030872 |
| 2003-06 | NP-20 | NP-030280 | 418 | 1 | Registratin Event - Shortend | 5.4.0 | 5.5.0 | N1-030844 |
| 2003-06 | NP-20 | NP-030280 | 419 | 1 | HSS / S-CSCF text relating to user deregistration | 5.4.0 | 5.5.0 | N1-030845 |
| 2003-06 | NP-20 | NP-030280 | 421 | | Handling of unknown methods at the P-CSCF | 5.4.0 | 5.5.0 | N1-030743 |
| 2003-06 | NP-20 | NP-030280 | 422 | 1 | Definitions and abbreviations update | 5.4.0 | 5.5.0 | N1-030870 |
| 2003-06 | NP-20 | NP-030280 | 423 | | Removal of hanging paragraph | 5.4.0 | 5.5.0 | N1-030752 |
| 2003-06 | NP-20 | NP-030280 | 424 | | Access network charging information | 5.4.0 | 5.5.0 | N1-030753 |
| 2003-06 | NP-20 | NP-030280 | 425 | 1 | UE procedure tidyup | 5.4.0 | 5.5.0 | N1-030871 |
| 2003-06 | NP-20 | NP-030281 | 426 | | P-CSCF procedure tidyup | 5.4.0 | 5.5.0 | N1-030755 |
| 2003-06 | NP-20 | NP-030281 | 427 | | I-CSCF procedure tidyup | 5.4.0 | 5.5.0 | N1-030756 |
| 2003-06 | NP-20 | NP-030281 | 428 | | S-CSCF procedure tidyup | 5.4.0 | 5.5.0 | N1-030757 |
| 2003-06 | NP-20 | NP-030281 | 429 | | BGCF procedure tidyup | 5.4.0 | 5.5.0 | N1-030758 |
| 2003-06 | NP-20 | NP-030281 | 430 | | AS procedure tidyup | 5.4.0 | 5.5.0 | N1-030759 |
| 2003-06 | NP-20 | NP-030281 | 431 | | MRFC procedure tidyup | 5.4.0 | 5.5.0 | N1-030760 |
| 2003-06 | NP-20 | NP-030281 | 434 | 1 | SDP procedure tidyup | 5.4.0 | 5.5.0 | N1-030852 |
| 2003-06 | NP-20 | NP-030281 | 438 | 2 | Profile Tables – Further Corrections | 5.4.0 | 5.5.0 | N1-030935 |
| 2003-06 | NP-20 | NP-030281 | 439 | 3 | AS's subscription for the registration state event package | 5.4.0 | 5.5.0 | N1-030940 |
| 2003-06 | NP-20 | NP-030281 | 440 | | Temporary Public User Identity in re- and de-REGISTER requests | 5.4.0 | 5.5.0 | N1-030792 |
| 2003-09 | NP-21 | NP-030412 | 444 | 2 | All non-REGISTER requests must be integrity protected | 5.5.0 | 5.6.0 | N1-031328 |
| 2003-09 | NP-21 | NP-030412 | 445 | | Download of all service profiles linked to PUID being registered and implicitly registered | 5.5.0 | 5.6.0 | N1-031010 |
| 2003-09 | NP-21 | NP-030412 | 448 | 3 | Authentication at UE | 5.5.0 | 5.6.0 | N1-031326 |
| 2003-09 | NP-21 | NP-030412 | 449 | 1 | Nework authentication failure at the UE | 5.5.0 | 5.6.0 | N1-031242 |

| Change history | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Date | TSG # | TSG Doc. | CR | Rev | Subject/Comment | Old | New | WG doc |
| 2003-09 | NP-21 | NP-030412 | 451 | 3 | Handling of security association | 5.5.0 | 5.6.0 | N1-031327 |
| 2003-09 | NP-21 | NP-030412 | 452 | 1 | Re-authentication timer at S-CSCF | 5.5.0 | 5.6.0 | N1-031274 |
| 2003-09 | NP-21 | NP-030412 | 455 | 2 | Authentication failure at S-CSCF | 5.5.0 | 5.6.0 | N1-031285 |
| 2003-09 | NP-21 | NP-030413 | 456 | 2 | Subscription termination sent by the S-CSCF | 5.5.0 | 5.6.0 | N1-031276 |
| 2003-09 | NP-21 | NP-030413 | 457 | | Subscription termination at the P-CSCF | 5.5.0 | 5.6.0 | N1-031032 |
| 2003-09 | NP-21 | NP-030413 | 458 | | Network -initiated deregistration at P-CSCF | 5.5.0 | 5.6.0 | N1-031033 |
| 2003-09 | NP-21 | NP-030349 | 459 | 2 | Notification about registration status at AS | 5.5.0 | 5.6.0 | |
| 2003-09 | NP-21 | NP-030413 | 461 | 1 | Service profile | 5.5.0 | 5.6.0 | N1-031233 |
| 2003-09 | NP-21 | NP-030413 | 466 | 1 | Requirements on Preconditions | 5.5.0 | 5.6.0 | N1-031246 |
| 2003-09 | NP-21 | NP-030413 | 467 | 1 | Call forwarding cleanup | 5.5.0 | 5.6.0 | N1-031238 |
| 2003-09 | NP-21 | NP-030413 | 468 | | Update of references | 5.5.0 | 5.6.0 | N1-031094 |
| 2003-09 | NP-21 | NP-030414 | 470 | 1 | Adding P-Asserted-Identity headers to NE initiated subscriptions | 5.5.0 | 5.6.0 | N1-031314 |
| 2003-09 | NP-21 | NP-030414 | 479 | 1 | Replace USIM by ISIM for user identity storage | 5.5.0 | 5.6.0 | N1-031247 |
| 2003-09 | NP-21 | NP-030414 | 481 | 1 | 24.229 R5 CR: Corrections to Profile Tables | 5.5.0 | 5.6.0 | N1-031248 |
| 2003-09 | NP-21 | NP-030414 | 482 | | 24.229 R5 CR: Setting of SUBSCRIBE exipiration time | 5.5.0 | 5.6.0 | N1-031140 |
| 2003-09 | NP-21 | NP-030414 | 483 | 3 | 24.229 R5 CR: Alignment of IMS Compression with RFC 3486 | 5.5.0 | 5.6.0 | N1-031335 |
| 2003-09 | NP-21 | NP-030418 | 465 | 1 | Alignment with TS for policy control over Gq interface | 5.6.0 | 6.0.0 | N1-031267 |
| 2003-09 | NP-21 | NP-030418 | 472 | 1 | I-CSCF procedures for openness | 5.6.0 | 6.0.0 | N1-031304 |
| 2003-09 | NP-21 | NP-030433 | 473 | 3 | Registration from multiple terminals and forking | 5.6.0 | 6.0.0 | |
| 2003-09 | NP-21 | NP-030419 | 480 | 3 | Access Independent IMS | 5.6.0 | 6.0.0 | N1-031333 |
| 2003-12 | NP-22 | NP-030482 | 487 | 1 | Registration amendments in profile | 6.0.0 | 6.1.0 | N1-031627 |
| 2003-12 | NP-22 | NP-030482 | 489 | | Privacy considerations for the UE | 6.0.0 | 6.1.0 | N1-031351 |
| 2003-12 | NP-22 | NP-030476 | 493 | | INVITE dialog amendments in profile | 6.0.0 | 6.1.0 | N1-031359 |
| 2003-12 | NP-22 | NP-030482 | 494 | | Correction of I-CSCF handling of multiple private user identities with same public user identity | 6.0.0 | 6.1.0 | N1-031375 |
| 2003-12 | NP-22 | NP-030476 | 496 | 1 | P-Asserted-Identity in SUBSCRIBE requests | 6.0.0 | 6.1.0 | N1-031632 |
| 2003-12 | NP-22 | NP-030482 | 497 | | Addition of reference to Gq interface | 6.0.0 | 6.1.0 | N1-031378 |
| 2003-12 | NP-22 | NP-030476 | 503 | 2 | Update of HSS information at deregistration | 6.0.0 | 6.1.0 | N1-031720 |
| 2003-12 | NP-22 | NP-030482 | 507 | | Unavailable definitions | 6.0.0 | 6.1.0 | N1-031392 |
| 2003-12 | NP-22 | NP-030476 | 509 | | Reference corrections | 6.0.0 | 6.1.0 | N1-031394 |
| 2003-12 | NP-22 | NP-030484 | 510 | 1 | UICC related changes for IMS commonality and interoperability | 6.0.0 | 6.1.0 | N1-031682 |
| 2003-12 | NP-22 | NP-030484 | 511 | | Interoperability and commonality; definition of scope | 6.0.0 | 6.1.0 | N1-031427 |
| 2003-12 | NP-22 | NP-030484 | 512 | | Interoperability and commonality; addition of terminology | 6.0.0 | 6.1.0 | N1-031428 |
| 2003-12 | NP-22 | NP-030484 | 513 | | Interoperability and commonality; media grouping | 6.0.0 | 6.1.0 | N1-031429 |

| Change history | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Date** | **TSG #** | **TSG Doc.** | **CR** | **Rev** | **Subject/Comment** | **Old** | **New** | **WG doc** |
| 2003-12 | NP-22 | NP-030484 | 515 | | Interoperability and commonality; charging information | 6.0.0 | 6.1.0 | N1-031431 |
| 2003-12 | NP-22 | NP-030482 | 518 | 1 | Profile support of RFC 3326: The Reason Header Field for the Session Initiation Protocol | 6.0.0 | 6.1.0 | N1-031681 |
| 2003-12 | NP-22 | NP-030482 | 519 | | Profile support of RFC 3581: An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing | 6.0.0 | 6.1.0 | N1-031439 |
| 2003-12 | NP-22 | NP-030484 | 522 | 1 | Clause 9 restructuring | 6.0.0 | 6.1.0 | N1-031684 |
| 2003-12 | NP-22 | NP-030477 | 524 | 2 | Correct use of RAND during re-synchronisation failures | 6.0.0 | 6.1.0 | N1-031712 |
| 2003-12 | NP-22 | NP-030478 | 526 | 1 | Correction to description or RES/XRES usage | 6.0.0 | 6.1.0 | N1-031617 |
| 2003-12 | NP-22 | NP-030483 | 529 | | Corrections on charging specification number | 6.0.0 | 6.1.0 | N1-031469 |
| 2003-12 | NP-22 | NP-030581 | 531 | 3 | Corrections on ICID for REGISTER | 6.0.0 | 6.1.0 | |
| 2003-12 | NP-22 | NP-030478 | 543 | 1 | Correction of user initiated re-registration | 6.0.0 | 6.1.0 | N1-031619 |
| 2003-12 | NP-22 | NP-030483 | 551 | 1 | IMS trust domain in Rel 6 | 6.0.0 | 6.1.0 | N1-031622 |
| 2003-12 | NP-22 | NP-030478 | 556 | 1 | P-CSCF and UE handling of Security Associations | 6.0.0 | 6.1.0 | N1-031624 |
| 2003-12 | NP-22 | NP-030483 | 560 | 2 | SDP offer handling in SIP responses in S-CSCF and P-CSCF | 6.0.0 | 6.1.0 | N1-031727 |
| 2003-12 | NP-22 | NP-030483 | 564 | 1 | SIP compression | 6.0.0 | 6.1.0 | N1-031705 |
| 2003-12 | NP-22 | NP-030478 | 566 | | Sending challenge | 6.0.0 | 6.1.0 | N1-031580 |
| 2003-12 | NP-22 | NP-030480 | 568 | 2 | Reg-await-auth timer value | 6.0.0 | 6.1.0 | N1-031716 |
| 2003-12 | NP-22 | NP-030480 | 571 | 1 | Network initiated deregistration | 6.0.0 | 6.1.0 | N1-031707 |
| 2003-12 | NP-22 | NP-030483 | 572 | | Text harmonisation with 3GPP2 | 6.0.0 | 6.1.0 | N1-031589 |
| 2003-12 | NP-22 | NP-030483 | 573 | 1 | Procedures in the absence of UICC | 6.0.0 | 6.1.0 | N1-031680 |
| 2003-12 | NP-22 | NP-030483 | 575 | 1 | P-Access-Network-Info changes | 6.0.0 | 6.1.0 | N1-031683 |
| 2004-03 | NP-23 | NP-040027 | 488 | 3 | Completion of major capabilities table in respect of privacy | 6.1.0 | 6.2.0 | N1-040406 |
| 2004-03 | NP-23 | NP-040027 | 499 | 5 | P-CSCF integrity protection | 6.1.0 | 6.2.0 | N1-040500 |
| 2004-03 | NP-23 | NP-040032 | 578 | 1 | UE requesting no-fork | 6.1.0 | 6.2.0 | N1-040184 |
| 2004-03 | NP-23 | NP-040032 | 579 | 1 | Inclusion of caller preferences into profile | 6.1.0 | 6.2.0 | N1-040284 |
| 2004-03 | NP-23 | NP-040027 | 586 | 1 | Network-initiated re-authentication | 6.1.0 | 6.2.0 | N1-040391 |
| 2004-03 | NP-23 | NP-040032 | 588 | 1 | Re-authentication - Abnormal cases | 6.1.0 | 6.2.0 | N1-040393 |
| 2004-03 | NP-23 | NP-040027 | 592 | 1 | Integrity protected correction | 6.1.0 | 6.2.0 | N1-040398 |
| 2004-03 | NP-23 | NP-040032 | 596 | 1 | Sec-agree parameter in "Proxy-Require" header | 6.1.0 | 6.2.0 | N1-040400 |
| 2004-03 | NP-23 | NP-040027 | 600 | 2 | Handling of record-route in target refresh and subsequent request | 6.1.0 | 6.2.0 | N1-040481 |
| 2004-03 | NP-23 | NP-040035 | 603 | | Cleanup for IP-CAN and GPRS | 6.1.0 | 6.2.0 | N1-040304 |
| 2004-03 | NP-23 | NP-040032 | 604 | | Forking in S-CSCF | 6.1.0 | 6.2.0 | N1-040325 |
| 2004-03 | NP-23 | NP-040108 | 605 | 3 | Determination of S-CSCF role | 6.1.0 | 6.2.0 | |
| 2004-03 | NP-23 | NP-040134 | 608 | 3 | Unprotected deregistration | 6.1.0 | 6.2.0 | |

| Change history | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Date** | **TSG #** | **TSG Doc.** | **CR** | **Rev** | **Subject/Comment** | **Old** | **New** | **WG doc** |
| 2004-03 | NP-23 | NP-040029 | 610 | | Sending authentication challenge | 6.1.0 | 6.2.0 | N1-040331 |
| 2004-03 | NP-23 | NP-040033 | 613 | | Reference to PDF operation | 6.1.0 | 6.2.0 | N1-040334 |
| 2004-03 | NP-23 | NP-040029 | 615 | 1 | Support of MESSAGE (Profile Tables) | 6.1.0 | 6.2.0 | N1-040466 |
| 2004-03 | NP-23 | NP-040033 | 616 | 2 | Introduction of PSI Routing to 24.229 | 6.1.0 | 6.2.0 | N1-040487 |
| 2004-03 | NP-23 | NP-040033 | 617 | 1 | P-CSCF Re-selection | 6.1.0 | 6.2.0 | N1-040463 |
| 2004-03 | NP-23 | NP-040033 | 618 | | I-CSCF does not re-select S-CSCF during re-registration | 6.1.0 | 6.2.0 | N1-040344 |
| 2004-03 | NP-23 | NP-040033 | 620 | 1 | Handling of media authorization token due to messaging | 6.1.0 | 6.2.0 | N1-040430 |
| 2004-06 | NP-24 | NP-040191 | 621 | 2 | Forking requests terminating at the served user | 6.2.0 | 6.3.0 | N1-040739 |
| 2004-06 | NP-24 | NP-040191 | 624 | 1 | Abbreviations | 6.2.0 | 6.3.0 | N1-040691 |
| 2004-06 | NP-24 | NP-040191 | 625 | 5 | Removal of restriction for multiple SIP sessions on a single PDP context | 6.2.0 | 6.3.0 | N1-041053 |
| 2004-06 | NP-24 | NP-040191 | 626 | 3 | Record route in S-CSCF | 6.2.0 | 6.3.0 | N1-041061 |
| 2004-06 | NP-24 | NP-040189 | 627 | 3 | Correction of reception of media authorization token | 6.2.0 | 6.3.0 | N1-040994 |
| 2004-06 | NP-24 | NP-040191 | 628 | 3 | Introduction of PSI Routing to 24.229 | 6.2.0 | 6.3.0 | N1-041059 |
| 2004-06 | NP-24 | NP-040198 | 629 | 2 | Addition of PRESNC material | 6.2.0 | 6.3.0 | N1-040996 |
| 2004-06 | NP-24 | NP-040189 | 631 | 1 | Missing statements regarding P-Charging-Function-Addresses header | 6.2.0 | 6.3.0 | N1-040987 |
| 2004-06 | NP-24 | NP-040191 | 634 | 1 | Multiple registrations | 6.2.0 | 6.3.0 | N1-041054 |
| 2004-06 | NP-24 | NP-040192 | 635 | 1 | Network-initiated deregistration | 6.2.0 | 6.3.0 | N1-041055 |
| 2004-06 | NP-24 | NP-040192 | 636 | | Network-initiated re-authentication | 6.2.0 | 6.3.0 | N1-040778 |
| 2004-06 | NP-24 | NP-040192 | 637 | 1 | Mobile-initiated deregistration | 6.2.0 | 6.3.0 | N1-041056 |
| 2004-06 | NP-24 | NP-040192 | 638 | 1 | Notification about registration state | 6.2.0 | 6.3.0 | N1-041057 |
| 2004-06 | NP-24 | NP-040189 | 642 | 3 | Syntax of the extension to the P-Charging-Vector header field | 6.2.0 | 6.3.0 | N1-041100 |
| 2004-06 | NP-24 | NP-040192 | 643 | 2 | Session Timer | 6.2.0 | 6.3.0 | N1-041095 |
| 2004-06 | NP-24 | NP-040193 | 644 | 3 | Session initiation without preconditions | 6.2.0 | 6.3.0 | N1-041096 |
| 2004-06 | NP-24 | NP-040192 | 645 | 1 | IMS Conferencing: Inclusion of Profile Tables to TS 24.229 | 6.2.0 | 6.3.0 | N1-041015 |
| 2004-06 | NP-24 | NP-040189 | 649 | 1 | Revisions due to published version of draft-ietf-sipping-reg-event | 6.2.0 | 6.3.0 | N1-040992 |
| 2004-06 | NP-24 | NP-040198 | 652 | | Creation of separate event package table for UA role | 6.2.0 | 6.3.0 | N1-041066 |
| 2004-09 | NP-25 | NP-040380 | 658 | | Correction of User identity verification at the AS | 6.3.0 | 6.4.0 | N1-041344 |
| 2004-09 | NP-25 | NP-040381 | 666 | 1 | NOTIFY requests | 6.3.0 | 6.4.0 | N1-041586 |
| 2004-09 | NP-25 | NP-040381 | 654 | 4 | Callee capabilities and Registration | 6.3.0 | 6.4.0 | N1-041315 |
| 2004-09 | NP-25 | NP-040381 | 668 | 2 | Network deregistration | 6.3.0 | 6.4.0 | N1-041614 |
| 2004-09 | NP-25 | NP-040381 | 682 | 1 | SDP parameters received by the S-CSCF and the P-CSCF in the 200 OK message | 6.3.0 | 6.4.0 | N1-041592 |
| 2004-09 | NP-25 | NP-040381 | 661 | 1 | Call Release | 6.3.0 | 6.4.0 | N1-041589 |

| Change history | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Date | TSG # | TSG Doc. | CR | Rev | Subject/Comment | Old | New | WG doc |
| 2004-09 | NP-25 | NP-040381 | 659 | | Multiple public ID registration | 6.3.0 | 6.4.0 | N1-041350 |
| 2004-09 | NP-25 | NP-040381 | 660 | | Standalone transactions | 6.3.0 | 6.4.0 | N1-041351 |
| 2004-09 | NP-25 | NP-040381 | 663 | | Unprotected REGISTER | 6.3.0 | 6.4.0 | N1-041354 |
| 2004-09 | NP-25 | NP-040381 | 662 | 1 | Session timer | 6.3.0 | 6.4.0 | N1-041590 |
| 2004-09 | NP-25 | NP-040381 | 665 | | Contact in SUBSCRIBE request | 6.3.0 | 6.4.0 | N1-041372 |
| 2004-09 | NP-25 | NP-040381 | 650 | 2 | Support of draft-ietf-sip-replaces | 6.3.0 | 6.4.0 | N1-041391 |
| 2004-09 | NP-25 | NP-040381 | 657 | 1 | Support of draft-ietf-sip-join | 6.3.0 | 6.4.0 | N1-041393 |
| 2004-09 | NP-25 | NP-040381 | 656 | 1 | Support of draft-ietf-sip-referredby | 6.3.0 | 6.4.0 | N1-041263 |
| 2004-09 | NP-25 | NP-040381 | 678 | | Support of TLS | 6.3.0 | 6.4.0 | N1-041462 |
| 2004-09 | NP-25 | NP-040381 | 688 | 2 | Filtering of the P-Access-Network-Info header by the S-CSCF and privacy rules | 6.3.0 | 6.4.0 | N1-041641 |
| 2004-09 | NP-25 | NP-040382 | 692 | 2 | Ipv6 IPv4 interworking | 6.3.0 | 6.4.0 | N1-041630 |
| 2004-09 | NP-25 | NP-040383 | 689 | 2 | Addition of session set-up not requiring preconditions and reliable transport of provisional responses. | 6.3.0 | 6.4.0 | N1-041632 |
| 2004-09 | NP-25 | NP-040385 | 697 | | Missing value for the event attribute within the <contact> element of NOTIFY body | 6.3.0 | 6.4.0 | N1-041540 |
| 2004-09 | NP-25 | NP-040385 | 698 | | HSS initiated deregistration | 6.3.0 | 6.4.0 | N1-041549 |
| 2004-09 | NP-25 | NP-040385 | 673 | | Syntax correction for the P-Charging-Vector header | 6.3.0 | 6.4.0 | N1-041434 |
| 2004-09 | NP-25 | NP-040385 | 699 | 1 | Network initiated deregistration upon UE roaming and registration to a new network | 6.3.0 | 6.4.0 | N1-041629 |
| 2004-12 | NP-26 | NP-040506 | 651 | 4 | Downloading the user profile based on User-Data-Request-Type | 6.4.0 | 6.5.0 | N1-042031 |
| 2004-12 | NP-26 | NP-040506 | 703 | 2 | SDP Encryption | 6.4.0 | 6.5.0 | N1-042095 |
| 2004-12 | NP-26 | NP-040506 | 704 | 1 | RTCP streams | 6.4.0 | 6.5.0 | N1-042019 |
| 2004-12 | NP-26 | NP-040506 | 709 | | Contact in 200(OK) response | 6.4.0 | 6.5.0 | N1-041725 |
| 2004-12 | NP-26 | NP-040506 | 710 | 1 | P-Access-Network-Info header | 6.4.0 | 6.5.0 | N1-042020 |
| 2004-12 | NP-26 | NP-040506 | 711 | 1 | P-Called-Party-ID header | 6.4.0 | 6.5.0 | N1-041954 |
| 2004-12 | NP-26 | NP-040506 | 713 | 1 | IMS-ALG routing | 6.4.0 | 6.5.0 | N1-042021 |
| 2004-12 | NP-26 | NP-040506 | 714 | 1 | Public User Identity | 6.4.0 | 6.5.0 | N1-042022 |
| 2004-12 | NP-26 | NP-040506 | 715 | 1 | "Pres" and "im" URIs | 6.4.0 | 6.5.0 | N1-042023 |
| 2004-12 | NP-26 | NP-040502 | 723 | 1 | Correction Term IOI handling | 6.4.0 | 6.5.0 | N1-041956 |
| 2004-12 | NP-26 | NP-040502 | 725 | 1 | Request handling in S-CSCF originating case | 6.4.0 | 6.5.0 | N1-041958 |
| 2004-12 | NP-26 | NP-040502 | 727 | 1 | Request handling in S-CSCF - terminating case | 6.4.0 | 6.5.0 | N1-041960 |
| 2004-12 | NP-26 | NP-040506 | 728 | | SBLP and non-realtime PDP contexts | 6.4.0 | 6.5.0 | N1-041797 |
| 2004-12 | NP-26 | NP-040590 | 730 | 2 | Reference updates | 6.4.0 | 6.5.0 | N1-042085 |
| 2004-12 | NP-26 | NP-040590 | 733 | 3 | Support for extended SigComp | 6.4.0 | 6.5.0 | N1-042117 |
| 2004-12 | NP-26 | NP-040590 | 734 | 2 | Correction to subclause 5.1.3 of TS 24,229 | 6.4.0 | 6.5.0 | N1-042120 |
| 2004-12 | NP-26 | NP-040590 | 735 | 1 | Correction to subclause 5.1.4.1.2.3 of TS 24,.229 | 6.4.0 | 6.5.0 | N1-042084 |
| 2004-12 | NP-26 | NP-040502 | 738 | 1 | Population of Via header when using REGISTER | 6.4.0 | 6.5.0 | N1-041962 |

| Change history | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Date | TSG # | TSG Doc. | CR | Rev | Subject/Comment | Old | New | WG doc |
| | | | | | method | | | |
| 2004-12 | NP-26 | NP-040590 | 739 | | Tel-URI related reference updates | 6.4.0 | 6.5.0 | N1-041869 |
| 2004-12 | NP-26 | NP-040590 | 741 | 1 | Throttling | 6.4.0 | 6.5.0 | N1-042086 |
| 2004-12 | NP-26 | NP-040590 | 742 | | Editorial correction resulting from CR665 | 6.4.0 | 6.5.0 | N1-041881 |
| 2004-12 | NP-26 | NP-040590 | 743 | | Unprotected REGISTER corrections | 6.4.0 | 6.5.0 | N1-041882 |
| 2004-12 | NP-26 | NP-040590 | 744 | 1 | Corrections to receiving SDP offer in 200 (OK) response | 6.4.0 | 6.5.0 | N1-042087 |
| 2004-12 | NP-26 | NP-040590 | 745 | 1 | Privacy corrections | 6.4.0 | 6.5.0 | N1-042085 |
| 2004-12 | NP-26 | NP-040590 | 747 | 2 | Syntax of the P-Charging-Vector | 6.4.0 | 6.5.0 | N1-042105 |
| 2004-12 | NP-26 | NP-040590 | 752 | 2 | Unavailability of the access-network-charging-info when the session is established without SBLP | 6.4.0 | 6.5.0 | N1-042106 |
| 2004-12 | NP-26 | NP-040590 | 753 | 1 | SIP messages carrying the access-network-charging-info for sessions without preconditions | 6.4.0 | 6.5.0 | N1-042089 |
| 2004-12 | NP-26 | NP-040590 | 755 | 1 | Network-initiated deregistration for multiple UEs sharing the same user public identity and for the old contact information of a roaming UE registered in a new network | 6.4.0 | 6.5.0 | N1-042090 |
| 2004-12 | NP-26 | NP-040502 | 765 | 1 | Interaction between S-CSCF and HSS in Network initiated deregistration procedure | 6.4.0 | 6.5.0 | N1-041966 |
| 2004-12 | NP-26 | NP-040502 | 768 | 1 | Downloading of user profile | 6.4.0 | 6.5.0 | N1-042103 |
| 2005-01 | | | | | Fix Word problem | 6.5.0 | 6.5.1 | |
| 2005-03 | NP-27 | NP-050069 | 839 | | Filter criteria matching and generation of third-party REGISTER request for network-initiated deregistration | 5.11.1 | 5.12.0 | N1-050220 |
| 2005-03 | NP-27 | NP-050069 | 785 | | Deregistration effect on active sessions | 6.5.1 | 6.6.0 | N1-050052 |
| 2005-03 | NP-27 | NP-050069 | 784 | | Deregistration effect on active sessions | 5.11.1 | 5.12.0 | N1-050051 |
| 2005-03 | NP-27 | NP-050069 | 809 | 1 | IOI storage at MGCF | 5.11.1 | 5.12.0 | N1-050295 |
| 2005-03 | NP-27 | NP-050069 | 840 | | Filter criteria matching and generation of third-party REGISTER request for network-initiated deregistration | 6.5.1 | 6.6.0 | N1-050221 |
| 2005-03 | NP-27 | NP-050069 | 806 | 1 | Use of original dialog identifier at AS | 6.5.1 | 6.6.0 | N1-050292 |
| 2005-03 | NP-27 | NP-050069 | 807 | 2 | Checking Request-URI for terminating requests at the S-CSCF | 5.11.1 | 5.12.0 | N1-050401 |
| 2005-03 | NP-27 | NP-050069 | 805 | 1 | Use of original dialog identifier at AS | 5.11.1 | 5.12.0 | N1-050291 |
| 2005-03 | NP-27 | NP-050069 | 808 | 2 | Checking Request-URI for terminating requests at the S-CSCF | 6.5.1 | 6.6.0 | N1-050402 |
| 2005-03 | NP-27 | NP-050069 | 810 | 1 | IOI storage at MGCF | 6.5.1 | 6.6.0 | N1-050296 |
| 2005-03 | NP-27 | NP-050073 | 794 | | RFC 3966 | 6.5.1 | 6.6.0 | N1-050080 |
| 2005-03 | NP-27 | NP-050073 | 848 | 1 | Removal of I-CSCF normative requirement on Cx interface | 6.5.1 | 6.6.0 | N1-050299 |
| 2005-03 | NP-27 | NP-050073 | 841 | | Filtering of the P-Access-Network-Info header by the S-CSCF and privacy rules | 6.5.1 | 6.6.0 | N1-050225 |
| 2005-03 | NP-27 | NP-050073 | 817 | | Editorial corrections | 6.5.1 | 6.6.0 | N1-050129 |
| 2005-03 | NP-27 | NP-050073 | 786 | 1 | Cleanups resulting from CR changes for last version | 6.5.1 | 6.6.0 | N1-050324 |

| Change history | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Date | TSG # | TSG Doc. | CR | Rev | Subject/Comment | Old | New | WG doc |
| 2005-03 | NP-27 | NP-050073 | 821 | 1 | Handling topmost Route header at the P-CSCF | 6.5.1 | 6.6.0 | N1-050297 |
| 2005-03 | NP-27 | NP-050073 | 790 | | Registration - Abnormal Case | 6.5.1 | 6.6.0 | N1-050076 |
| 2005-03 | NP-27 | NP-050074 | 832 | 1 | Corrections to the tables for "PUBLISH" | 6.5.1 | 6.6.0 | N1-050341 |
| 2005-03 | NP-27 | NP-050074 | 822 | 1 | Corrections to the UE tables for "major capabilities" | 6.5.1 | 6.6.0 | N1-050332 |
| 2005-03 | NP-27 | NP-050074 | 825 | 1 | Corrections to the UE tables for "ACK" | 6.5.1 | 6.6.0 | N1-050334 |
| 2005-03 | NP-27 | NP-050074 | 826 | 1 | Corrections to the tables for "CANCEL" | 6.5.1 | 6.6.0 | N1-050335 |
| 2005-03 | NP-27 | NP-050074 | 827 | 1 | Corrections to the tables for "INVITE" | 6.5.1 | 6.6.0 | N1-050336 |
| 2005-03 | NP-27 | NP-050074 | 828 | 1 | Corrections to the tables for "MESSAGE" | 6.5.1 | 6.6.0 | N1-050337 |
| 2005-03 | NP-27 | NP-050074 | 829 | 1 | Corrections to the tables for "NOTIFY" | 6.5.1 | 6.6.0 | N1-050338 |
| 2005-03 | NP-27 | NP-050074 | 830 | 1 | Corrections to the tables for "OPTIONS" | 6.5.1 | 6.6.0 | N1-050339 |
| 2005-03 | NP-27 | NP-050074 | 834 | 1 | Corrections to the tables for "REGISTER" | 6.5.1 | 6.6.0 | N1-050343 |
| 2005-03 | NP-27 | NP-050074 | 831 | 1 | Corrections to the tables for "PRACK" | 6.5.1 | 6.6.0 | N1-050340 |
| 2005-03 | NP-27 | NP-050074 | 833 | 1 | Corrections to the tables for "REFER" | 6.5.1 | 6.6.0 | N1-050342 |
| 2005-03 | NP-27 | NP-050074 | 835 | 1 | Corrections to the tables for "SUBSCRIBE" | 6.5.1 | 6.6.0 | N1-050344 |
| 2005-03 | NP-27 | NP-050074 | 836 | 1 | Corrections to the tables for "UPDATE" | 6.5.1 | 6.6.0 | N1-050345 |
| 2005-03 | NP-27 | NP-050074 | 837 | 1 | Corrections to the tables for SDP | 6.5.1 | 6.6.0 | N1-050346 |
| 2005-03 | NP-27 | NP-050074 | 824 | 1 | Removal of the UE table for 'status codes' | 6.5.1 | 6.6.0 | N1-050351 |
| 2005-03 | NP-27 | NP-050074 | 823 | 1 | Corrections to the tables for "BYE" | 6.5.1 | 6.6.0 | N1-050333 |
| 2005-03 | NP-27 | NP-050075 | 846 | 2 | Correction to the Registration procedure | 6.5.1 | 6.6.0 | N1-050413 |
| 2005-03 | NP-27 | NP-050075 | 850 | 1 | Addition of IMS-ALF to profile tables | 6.5.1 | 6.6.0 | N1-050348 |
| 2005-03 | NP-27 | NP-050075 | 851 | 2 | Press and im URIs in incoming requests | 6.5.1 | 6.6.0 | N1-050395 |
| 2005-03 | NP-27 | NP-050075 | 788 | 1 | MO - Calls to IPv4 SIP terminals | 6.5.1 | 6.6.0 | N1-050387 |
| 2005-03 | NP-27 | NP-050075 | 818 | 3 | Corrections to subclause 5.5 in TS 24.229 | 6.5.1 | 6.6.0 | N1-050414 |
| 2005-03 | NP-27 | NP-050075 | 801 | 3 | Default handling associated with the trigger at the S-CSCF | 6.5.1 | 6.6.0 | N1-050418 |
| 2005-03 | NP-27 | NP-050075 | 803 | 4 | Default handling associated with the trigger for third party registration | 6.5.1 | 6.6.0 | N1-050421 |
| 2005-03 | NP-27 | NP-050078 | 795 | 1 | Sip-profile package in major capabilities | 6.5.1 | 6.6.0 | N1-050306 |
| 2005-03 | NP-27 | NP-050127 | 849 | 2 | Corrections to addition of session set-up not requiring preconditions and reliable transport of provisional responses | 6.5.1 | 6.6.0 | |
| 2005-06 | CP-28 | CP-050059 | 879 | | Correction Reg-Await-Auth Timer | 6.6.0 | 6.7.0 | C1-050522 |
| 2005-06 | CP-28 | CP-050059 | 881 | | Security Association in P-CSCF | 6.6.0 | 6.7.0 | C1-050524 |
| 2005-06 | CP-28 | CP-050059 | 871 | 1 | Port 5060 | 6.6.0 | 6.7.0 | C1-050674 |
| 2005-06 | CP-28 | CP-050059 | 891 | 2 | SIP headers storage for P-CSCF initiated session release | 6.6.0 | 6.7.0 | C1-050777 |
| 2005-06 | CP-28 | CP-050059 | 921 | 1 | Correction of error in the specification of the extension to Authorization header | 6.6.0 | 6.7.0 | C1-050689 |
| 2005-06 | CP-28 | CP-050059 | 886 | 2 | Handling of P-Associated URI header | 6.6.0 | 6.7.0 | C1-050783 |

| Change history | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Date | TSG # | TSG Doc. | CR | Rev | Subject/Comment | Old | New | WG doc |
| 2005-06 | CP-28 | CP-050059 | 907 | 2 | Clarification to the procedures at the I-CSCF | 6.6.0 | 6.7.0 | C1-050785 |
| 2005-06 | CP-28 | CP-050061 | 894 | 1 | Re-registration failure | 6.6.0 | 6.7.0 | C1-050709 |
| 2005-06 | CP-28 | CP-050061 | 892 | | Completion of status-code tables in SIP profile | 6.6.0 | 6.7.0 | C1-050571 |
| 2005-06 | CP-28 | CP-050061 | 865 | 1 | Unsubscribe by P-CSCF | 6.6.0 | 6.7.0 | C1-050671 |
| 2005-06 | CP-28 | CP-050061 | 866 | 1 | Protected initial registration | 6.6.0 | 6.7.0 | C1-050708 |
| 2005-06 | CP-28 | CP-050061 | 916 | 1 | Clarify that S-CSCF shall support Supported and Require headers | 6.6.0 | 6.7.0 | C1-050684 |
| 2005-06 | CP-28 | CP-050061 | 862 | | Shared public user identities | 6.6.0 | 6.7.0 | C1-050599 |
| 2005-06 | CP-28 | CP-050061 | 860 | 1 | P-CSCF - routing of REGISTER requests | 6.6.0 | 6.7.0 | C1-050701 |
| 2005-06 | CP-28 | CP-050061 | 870 | 1 | Correction of table A.104A | 6.6.0 | 6.7.0 | C1-050711 |
| 2005-06 | CP-28 | CP-050061 | 887 | 1 | Contact address in REGISTER response | 6.6.0 | 6.7.0 | C1-050716 |
| 2005-06 | CP-28 | CP-050061 | 890 | 1 | P-CSCF Record-Route processing for target refresh requests/responses | 6.6.0 | 6.7.0 | C1-050717 |
| 2005-06 | CP-28 | CP-050061 | 893 | 1 | AS originated requests on behalf of PSI | 6.6.0 | 6.7.0 | C1-050719 |
| 2005-06 | CP-28 | CP-050061 | 896 | 1 | Routing PSI at terminating side | 6.6.0 | 6.7.0 | C1-050720 |
| 2005-06 | CP-28 | CP-050061 | 856 | 2 | Notification about registration state | 6.6.0 | 6.7.0 | C1-050789 |
| 2005-06 | CP-28 | CP-050061 | 861 | 3 | Registration failure at UE | 6.6.0 | 6.7.0 | C1-050790 |
| 2005-06 | CP-28 | CP-050061 | 899 | 2 | Correction of the references for the integration of resource management procedures | 6.6.0 | 6.7.0 | C1-050791 |
| 2005-06 | CP-28 | CP-050061 | 902 | 2 | Clarification on P-CSCF-intiated call release | 6.6.0 | 6.7.0 | C1-050792 |
| 2005-06 | CP-28 | CP-050061 | 863 | 3 | Error handling in UE in case of RFC 3524 | 6.6.0 | 6.7.0 | C1-050793 |
| 2005-06 | CP-28 | CP-050061 | 895 | 3 | UE registration failure because the selected S-CSCF is unreachable | 6.6.0 | 6.7.0 | C1-050802 |
| 2005-06 | CP-28 | CP-050061 | 787 | 6 | MT- SDP offer with IPv4 address. | 6.6.0 | 6.7.0 | C1-050794 |
| 2005-06 | CP-28 | CP-050061 | 858 | 1 | S-CSCF redirecting | 6.6.0 | 6.7.0 | C1-050700 |
| 2005-06 | CP-28 | CP-050064 | 872 | 2 | I-WLAN information for IMS | 6.6.0 | 6.7.0 | C1-050729 |
| 2005-09 | CP-29 | CP-050355 | 929 | 1 | Correction Profile Table A.119 | 6.7.0 | 6.8.0 | C1-051060 |
| 2005-09 | CP-29 | CP-050355 | 945 | | Public User identity in 3rd party REG | 6.7.0 | 6.8.0 | C1-050905 |
| 2005-09 | CP-29 | CP-050355 | 956 | 1 | Removal of Access Network Charging Information by the S-CSCF | 6.7.0 | 6.8.0 | C1-051080 |
| 2005-09 | CP-29 | CP-050355 | 964 | | Optional ccf | 6.7.0 | 6.8.0 | C1-050985 |
| 2005-09 | CP-29 | CP-050355 | 985 | | Contact header in REGISTER requests | 6.7.0 | 6.8.0 | C1-051176 |
| 2005-09 | CP-29 | CP-050358 | 943 | 2 | Modifications to 24.229 to allow multiple IPSec SA | 6.7.0 | 6.8.0 | C1-051210 |
| 2005-09 | CP-29 | CP-050359 | 931 | | SigComp-Corrections | 6.7.0 | 6.8.0 | C1-050876 |
| 2005-09 | CP-29 | CP-050359 | 961 | 1 | IETF reference corrections | 6.7.0 | 6.8.0 | C1-051073 |
| 2005-09 | CP-29 | CP-050359 | 967 | 1 | AS procedure correction | 6.7.0 | 6.8.0 | C1-051083 |
| 2005-12 | CP-30 | CP-050538 | 1048 | | Replace 'originated' with 'terminated' | 6.8.0 | 6.9.0 | C1-051478 |
| 2005-12 | CP-30 | CP-050538 | 1011 | 1 | Correction to section 5.4.3.2 of TS 24.229 | 6.8.0 | 6.9.0 | C1-051562 |
| 2005-12 | CP-30 | CP-050538 | 1070 | | Correction Syntax P-Charging Vector | 6.8.0 | 6.9.0 | C1-051507 |

| Change history | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Date | TSG # | TSG Doc. | CR | Rev | Subject/Comment | Old | New | WG doc |
| 2005-12 | CP-30 | CP-050538 | 1045 | 2 | Mobile originating call related requests | 6.8.0 | 6.9.0 | C1-051667 |
| 2005-12 | CP-30 | CP-050538 | 1025 | | Handling of P-Charging-Function-Address | 6.8.0 | 6.9.0 | C1-051423 |
| 2005-12 | CP-30 | CP-050541 | 1001 | 1 | Modification to the definition of Security Association | 6.8.0 | 6.9.0 | C1-051575 |
| 2005-12 | CP-30 | CP-050542 | 1028 | 1 | B2B UA AS handling | 6.8.0 | 6.9.0 | C1-041596 |
| 2005-12 | CP-30 | CP-050542 | 1058 | | Replace 'served' by 'Originating' UE | 6.8.0 | 6.9.0 | C1-051488 |
| 2005-12 | CP-30 | CP-050542 | 1053 | | Adjusting section reference in section 6.3 | 6.8.0 | 6.9.0 | C1-051483 |
| 2005-12 | CP-30 | CP-050542 | 1064 | 1 | Charging terms correction | 6.8.0 | 6.9.0 | C1-051617 |
| 2005-12 | CP-30 | CP-050542 | 1016 | | Correction to subclause 5.7.5.1. of TS 24229 | 6.8.0 | 6.9.0 | C1-051381 |
| 2005-12 | CP-30 | CP-050542 | 0993 | | cdma2000 | 6.8.0 | 6.9.0 | C1-051335 |
| 2005-12 | CP-30 | CP-050542 | 1072 | 5 | Short Session Setup in IMS | 6.8.0 | 6.9.0 | C1-051655 |
| 2005-12 | CP-30 | CP-050542 | 1004 | 2 | Refreshes of SUBSCRIBE to reg-event (Fix for Rel 6) | 6.8.0 | 6.9.0 | C1-051669 |
| 2005-12 | CP-30 | CP-050542 | 1063 | 2 | Correction to 3rd party registration procedures for SESSION_TERMINATED default handling | 6.8.0 | 6.9.0 | C1-051673 |
| 2005-12 | CP-30 | CP-050542 | 0981 | 3 | Access Type of P-Access-Network-Info header | 6.8.0 | 6.9.0 | C1-051674 |
| 2005-12 | CP-30 | CP-050542 | 1042 | | Correction of a reference in some tables in Appendix A | 6.8.0 | 6.9.0 | C1-051472 |
| 2006-03 | CP-31 | CP-060106 | 1113 | 1 | IMS AKA - content of initial authentication header | 6.9.0 | 6.10.0 | C1-060449 |
| 2006-03 | CP-31 | CP-060106 | 1116 | 1 | IMS AKA - SQN resync clarifications | 6.9.0 | 6.10.0 | C1-060452 |
| 2006-03 | CP-31 | CP-060111 | 1118 | 2 | IMS Short Session Setup - Clarifications | 6.9.0 | 6.10.0 | C1-060594 |
| 2006-03 | CP-31 | CP-060111 | 1128 | 2 | Tel URI | 6.9.0 | 6.10.0 | C1-060592 |
| 2006-03 | CP-31 | CP-060110 | 1131 | 1 | P-Asserted-Identity | 6.9.0 | 6.10.0 | C1-060475 |
| 2006-03 | CP-31 | CP-060110 | 1133 | - | Preconditions required | 6.9.0 | 6.10.0 | C1-060191 |
| 2006-03 | CP-31 | CP-060110 | 1135 | 1 | SDP answer | 6.9.0 | 6.10.0 | C1-060471 |
| 2006-03 | CP-31 | CP-060107 | 1141 | 1 | Support of call forwarding at the S-CSCF | 6.9.0 | 6.10.0 | C1-060462 |
| 2006-03 | CP-31 | CP-060107 | 1147 | 1 | UE processing 305 (Use Proxy) | 6.9.0 | 6.10.0 | C1-060506 |
| 2006-03 | CP-31 | CP-060110 | 1155 | 1 | Tables Change in Appendix A | 6.9.0 | 6.10.0 | C1-060477 |
| 2006-03 | CP-31 | CP-060107 | 1160 | 1 | DHCPv6 options for Domain Name Servers | 6.9.0 | 6.10.0 | C1-060455 |
| 2006-03 | CP-31 | CP-060107 | 1163 | 1 | Clarifications on P-CSCF discovery | 6.9.0 | 6.10.0 | C1-060458 |
| 2006-03 | CP-31 | CP-060106 | 1186 | - | Removal of Warning header non-compliance with RFC 3261 | 6.9.0 | 6.10.0 | C1-060327 |
| 2006-03 | CP-31 | CP-060111 | 1188 | 3 | Definition of principles for IOI exchange and storage | 6.9.0 | 6.10.0 | C1-060609 |
| 2006-03 | CP-31 | CP-060106 | 1203 | - | Syntax and operation for Security-Client, Security-Server and Security-Verify headers | 6.9.0 | 6.10.0 | C1-060386 |
| 2006-03 | CP-31 | CP-060110 | 1205 | - | Inclusion of Ma reference point | 6.9.0 | 6.10.0 | C1-060391 |
| 2006-03 | CP-31 | CP-060117 | 1209 | 1 | Coding of P-Access-Network-Info header for 3GPP2 IMS | 6.9.0 | 6.10.0 | C1-060493 |
| 2006-03 | CP-31 | CP-060111 | 1213 | 1 | Reference Update of TS24.229, Rel6 | 6.9.0 | 6.10.0 | C1-060482 |

# History

| Document history | | |
|---|---|---|
| V6.5.1 | January 2005 | Publication |
| V6.6.0 | March 2005 | Publication |
| V6.7.0 | June 2005 | Publication |
| V6.8.0 | September 2005 | Publication |
| V6.9.0 | December 2005 | Publication |
| V6.10.0 | March 2006 | Publication |